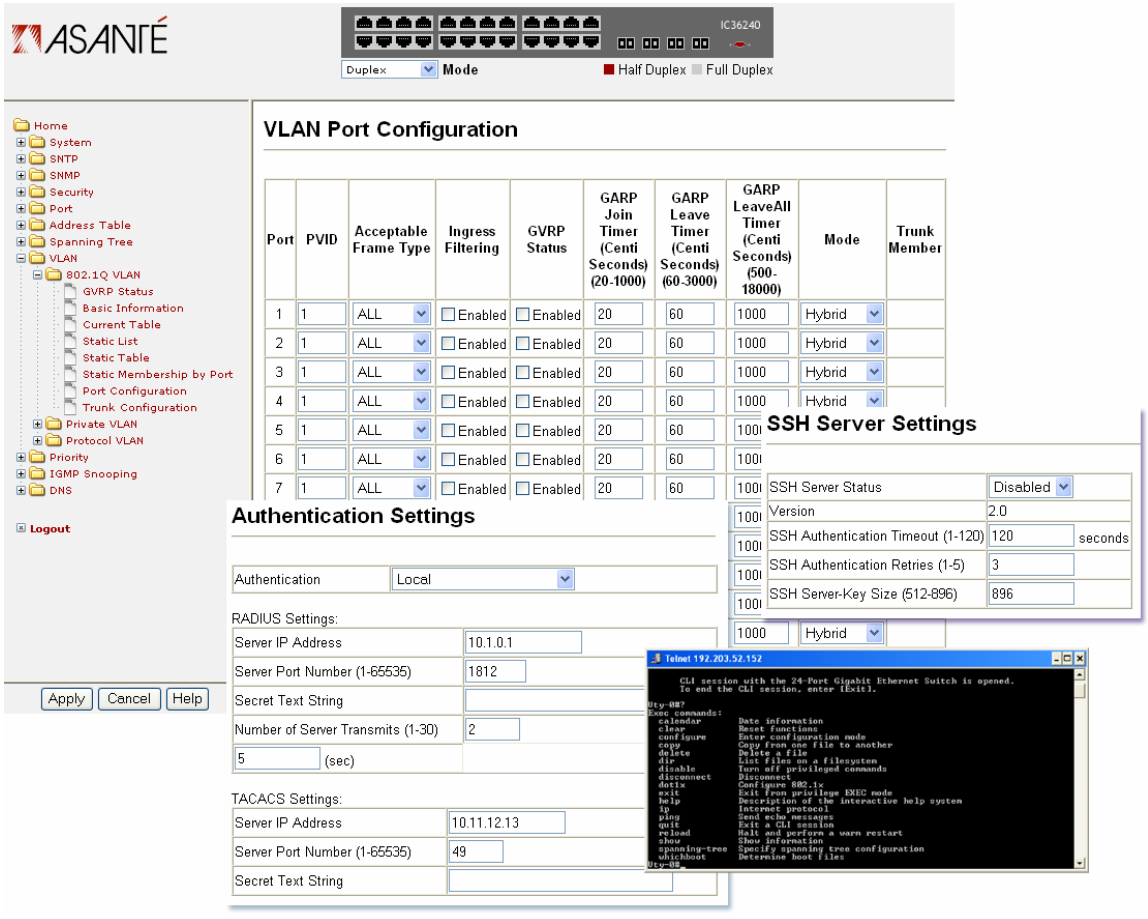
ASANTÉ



IntraCore® 36000 Series

Managed Gigabit Ethernet Switches

User's Manual

IntraCore 36000 Series
Managed Gigabit Ethernet Switches

User's Manual
Revision 1.0

Asanté Technologies, Inc.
821 Fox Lane
San Jose, CA 95131
USA

SALES

800-662-9686 Home/Office Solutions
800-303-9121 Enterprise Solutions
408-435-8388

TECHNICAL SUPPORT

801-566-8991: Worldwide
801-566-3787: Fax
www.asante.com/support
support@asante.com

[Default IP Address: 192.168.0.1]
[Default username: root]
[Default password: Asante]

Copyright © 2004 Asanté Technologies, Inc. All rights reserved. No part of this document, or any associated artwork, product design, or design concept may be copied or reproduced in whole or in part by any means without the express written consent of Asanté Technologies, Inc. Asanté and IntraCore are registered trademarks and the Asanté logo, AsantéCare, Auto-Uplink, and IntraCare are trademarks of Asanté Technologies, Inc. All other brand names or product names are trademarks or registered trademarks of their respective holders. All features and specifications are subject to change without prior notice.

Table of Contents

Table of Contents 3

Chapter 1: Introduction 16

1.1 Description of Software Features 16

1.2 System Defaults 19

Chapter 2: Initial Configuration 22

2.1 Connecting to the Switch 22

2.2 Connections 23

2.3 Setting a Password 24

2.4 Setting an IP Address 25

2.5 Enabling SNMP Management Access 28

2.6 Saving Configuration Settings 29

2.7 Managing System Files 29

2.8 Managing Firmware 30

2.9 Saving or Restoring Configuration Settings 31

2.10 Basic Management 33

Chapter 3: Configuring Global Settings 38

3.1 Configuring Spanning Tree 39

3.2 Configuring Interface Settings 44

3.3 Configuring Multiple Spanning Trees 46

Chapter 4: Configuring SNTP 53

4.1 SNTP Attributes 53

4.2 Setting the Time Zone 53

Chapter 5: Simple Network Management Protocol 55

5.1 Setting Community Access Strings 55

5.2 Specifying Trap Managers and Trap Types 56

Chapter 6: Configuring Security 57

6.1 Configuring User Accounts 57

6.2 Configuring Local/Remote Logon Authentication 57

6.3 Configuring HTTPS 59
6.4 Configuring the Secure Shell 61
6. 5 Configuring Port Security 65
6.6 Configuring 802.1x Port Authentication 67
6.7 Configuring Access Control Lists 74
6.8 Configuring IP Filters 83
Chapter 7: Configuring Ports 85
7.1 Displaying Connection Status 85
7.2 Configuring Interface Connections 87
7.3 Configuring Trunk Groups 89
7.4 Enabling LACP on Selected Ports 91
7.5 Setting Broadcast Storm Thresholds 98
7.6 Configuring Port Mirroring 100
7.7 Configuring Rate Limits 101
7.8 Showing Port Statistics 101
Chapter 8: Configuring Address Table Settings 106
8.1 Setting Static Addresses 106
8.2 Displaying the Dynamic Address Table 107
8.3 Changing the Aging Time 108
Chapter 9: Configuring Spanning Tree 109
Chapter 10: Configuring VLAN 112
10.1 Assigning Ports to VLANs 112
10.2 Configuring Private VLANs 121
10.3 Configuring Protocol-Based VLANs 122
Chapter 11: Configuring Packet Priority 125
11.1 Setting the Default Priority for Interfaces 125
11.2 Mapping CoS Values to Egress Queues 126
11.3 Selecting the Queue Mode 127
11.4 Setting the Service Weight for Traffic Classes 128

11.5 Selecting IP Precedence/DSCP Priority 130
11.6 Mapping CoS Values to ACLs 134
11.7 Changing Priorities Based on ACL Rules 135
Chapter 12: Layer 2 IGMP (Snooping and Query) 138
12.1 IGMP Multicast Filtering 138
Chapter 13: Configuring Domain Name Service 144
13.1 General DNS Server Parameters 144
13.2 Static DNS Host to Address Entries 145
13.3 Displaying the DNS Cache 147
Chapter 14: Using the Command Line Interface 148
14.1 Exec Commands 148
14.2 Configuration Commands 149
14.3 Command Groups 150
Chapter 15: Configuration Guide 152
15.1 Line Commands 152
15.2 General Commands 152
15.3 System Management Commands 153
15.4 Authentication Commands 159
15.5 Access Control List Commands 161
15.6 SNMP Commands 164
15.7 DHCP Commands 164
15.8 Interface Commands 165
15.9 Mirror Port Commands 166
15.10 Rate Limit Commands 166
15.11 Link Aggregation Commands 166
15.12 Address Table Commands 168
15.13 Spanning Tree Commands 168
15.14 VLAN Commands 169
15.15 GVRP and Bridge Extension Commands 171

15.16 Priority Commands 172
15.17 Multicast Filtering Commands 173
15.18 IP Interface Commands 175
Chapter 16: Command Reference 176
16.1 access-list ip 176
16.2 access-list ip mask-precedence 177
16.3 access-list mac 177
16.4 access-list mac mask-precedence 178
16.5 authentication dot1x default 179
16.6 authentication enable 180
16.7 authentication login 181
16.8 boot system 181
16.9 bridge-ext gvrp 182
16.10 calendar set 183
16.11 capabilities 184
16.12 channel-group 185
16.13 clear counters 185
16.14 clear dns cache 186
16.15 clear host 187
16.16 clear logging 187
16.17 clear mac-address-table dynamic 188
16.18 clock timezone 188
16.19 combo-forced-mode 189
16.20 configure 190
16.21 copy 190
16.22 databits 192
16.23 delete 193
16.24 delete public-key 194
16.25 description 194

16.26 dir 195
16.27 disable 196
16.28 disconnect 197
16.29 dot1x default 197
16.30 dot1x max-req 198
16.31 dot1x operation-mode 198
16.32 dot1x port-control 199
16.33 dot1x re-authenticate 199
16.34 dot1x re-authentication 200
16.35 dot1x timeout quiet-period 200
16.36 dot1x timeout re-authperiod 201
16..37 dot1x timeout tx-period 201
16.38 enable 202
16.39 enable password 203
16.40 end 203
16.41 exec-timeout 204
16.42 exit 205
16.43 flowcontrol 205
16.44 garp timer 206
16.45 hostname 207
16.46 interface 208
16.47 interface vlan 208
16.48 ip access-group 209
16.49 ip address 210
16.50 ip default-gateway 211
16.51 ip dhcp restart 211
16.52 ip domain-list 212
16.53 ip domain-lookup 213
16.54 ip domain-name 214

16.55 ip host 215
16.56 ip http port 216
16.57 ip http secure-port 216
16.58 ip http secure-server 217
16.59 ip http server 218
16.60 ip igmp snooping 219
16.61 ip igmp snooping querier 219
16.62 ip igmp snooping query-count 220
16.63 ip igmp snooping query-interval 221
16.64 ip igmp snooping query-max-response-time 221
16.65 ip igmp snooping router-port-expire-time 222
16.66 ip igmp snooping version 223
16.67 ip igmp snooping vlan mrouter 223
16.68 ip igmp snooping vlan static 224
16.69 ip name-server 225
16.70 ip ssh authentication-retries 226
16.71 ip ssh crypto host-key generate 226
16.72 ip ssh crypto zeroize 227
16.73 ip ssh save host-key 228
16.74 ip ssh server 228
16.75 ip ssh server-key size 229
16.76 ip ssh timeout 230
16.77 jumbo frame 231
16.78 lacp 231
16.79 lacp admin-key (Ethernet Interface) 232
16.80 lacp admin-key (Port Channel) 233
16.81 lacp port-priority 234
16.82 lacp system-priority 235
16.83 line 236

16.84 logging facility 236
16.85 logging history 237
16.86 logging host 238
16.87 logging on 239
16.88 logging sendmail 239
16.89 logging sendmail destination-email 240
16.90 logging sendmail host 240
16.91 logging sendmail level 241
16.92 logging sendmail source-email 242
16.93 logging trap 242
16.94 login 243
16.95 mac access-group 244
16.96 mac-address-table aging-time 244
16.97 mac-address-table static 245
16.98 management 246
16.99 map access-list ip 247
16.100 mask (IP ACL) 248
16.101 map access-list mac 251
16.102 map ip dscp (Global Configuration) 252
16.103 map ip dscp (Interface Configuration) 252
16.104 map ip port (Global Configuration) 254
16.105 map ip port (Interface Configuration) 254
16.106 map ip precedence (Global Configuration) 255
16.107 map ip precedence (Interface Configuration) 255
16.108 mask (MAC ACL) 256
16.109 match access-list ip 258
16.110 match access-list mac 259
16.111 max-hops 260
16.112 mst priority 260

16.113 mst vlan 261
16.114 name 262
16.115 negotiation 263
16.116 parity 263
16.117 password 264
16.118 password-thresh 265
16.119 permit, deny (Extended ACL) 266
16.120 permit, deny (MAC ACL) 268
16.121 permit, deny (Standard ACL) 270
16.122 ping 270
16.123 port security 272
16.124 prompt 273
16.125 protocol-vlan protocol-group (Configuring Groups) 274
16.126 protocol-vlan protocol-group (Configuring Interfaces) 274
16.127 pvlan 275
16.128 queue bandwidth 276
16.129 queue cos-map 277
16.130 queue mode 278
16.131 quit 278
16.132 radius-server host 279
16.133 radius-server key 279
16.134 radius-server port 280
16.135 radius-server retransmit 280
16.136 radius-server timeout 281
16.137 rate-limit 281
16.138 reload 282
16.139 revision 282
16.140 show access-group 283
16.141 show access-list 283

16.142 show access-list ip mask-precedence 284
16.143 show access-list mac mask-precedence 285
16.144 show bridge-ext 285
16.145 show calendar 286
16.146 show dns 286
16.147 show dns cache 287
16.148 show dot1x 287
16.149 show garp timer 290
16.150 show gvrp configuration 291
16.151 show history 291
16.152 show hosts 292
16.153 show interfaces counters 292
16.154 show interfaces protocol-vlan protocol-group 294
16.155 show interfaces status 294
16.156 show interfaces switchport 295
16.157 show ip access-group 297
16.158 show ip access-list 297
16.159 show ip igmp snooping 298
16.160 show ip igmp snooping mrouter 298
16.161 show ip interface 299
16.162 show ip redirects 300
16.163 show ip ssh 300
16.164 show lacp 300
16.165 show line 304
16.166 show logging 305
16.167 show logging sendmail 306
16.168 show mac access-group 307
16.169 show mac access-list 307
16.170 show mac-address-table 308

16.171 show mac-address-table aging-time 309
16.172 show mac-address-table multicast 309
16.173 show map access-list ip 310
16.174 show map access-list mac 311
16.175 show map ip dscp 311
16.176 show map ip port 312
16.177 show map ip precedence 313
16.178 show management 314
16.179 show marking 315
16.180 show port monitor 315
16.181 show protocol-vlan protocol-group 316
16.182 show public-key 317
16.183 show pvlan 318
16.184 show queue bandwidth 318
16.185 show queue cos-map 319
16.186 show queue mode 319
16.187 show radius-server 320
16.188 show running-config 320
16.189 show snmp 322
16.190 show sntp 323
16.191 show spanning-tree 323
16.192 show spanning-tree mst configuration 325
16.193 show ssh 325
16.194 show startup-config 327
16.195 show system 329
16.196 show tacacs-server 329
16.197 show users 330
16.198 show version 330
16.199 show vlan 331

16.200 shutdown 332
16.201 silent-time 332
16.202 snmp-server community 333
16.203 snmp-server contact 334
16.204 snmp-server enable traps 334
16.205 snmp-server host 335
16.206 snmp-server location 336
16.207 sntp broadcast client 337
16.208 sntp client 337
16.209 sntp poll 338
16.210 sntp server 339
16.211 spanning-tree 340
16.212 spanning-tree cost 340
16.213 spanning-tree edge-port 341
16.214 spanning-tree forward-time 342
16.215 spanning-tree hello-time 343
16.216 spanning-tree link-type 343
16.217 spanning-tree mst cost 344
16.218 spanning-tree mst port-priority 345
16.219 spanning-tree max-age 346
16.220 spanning-tree mode 347
16.221 spanning-tree mst configuration 348
16.222 spanning-tree pathcost method 349
16.223 spanning-tree portfast 349
16.224 spanning-tree port-priority 350
16.225 spanning-tree priority 351
16.226 spanning-tree spanning-disabled 351
16.227 spanning-tree transmission-limit 352
16.228 speed 353

16.229 speed-duplex 353
16.230 stopbits 354
16.231 switchport acceptable-frame-types 355
16.232 switchport allowed vlan 356
16.233 switchport broadcast packet-rate 357
16.234 switchport forbidden vlan 357
16.235 switchport gvrp 358
16.236 switchport ingress-filtering 359
16.237 switchport mode 359
16.238 switchport native vlan 360
16.239 switchport priority default 361
16.240 tacacs-server host 362
16.241 tacacs-server key 362
16.242 tacacs-server port 363
16.243 username 363
16.244 vlan database 364
16.245 vlan 365
16.246 whichboot 366
Appendix A: Web Browser Interface and Command Line Interface Overview 367
A.1 Navigating the Web Browser Interface 367
A.2 Improving Response Time 367
A.3 Configuration Options 367
A.4 Accessing the CLI 368
A.5 Console Connection 368
A.6 Telnet Connection 368
A.7 Entering Commands 369
Appendix B: Upgrading Firmware Through the Serial Port 373
B.1 Power Cycle the Switch. 373
Appendix C: Software Specifications 375

Appendix D: Troubleshooting and Pinouts 380

D.1 Troubleshooting Chart 380

D.2 Console Port Pin Assignments 380

Appendix E: FCC Compliance and Warranty Statements 381

E.1 FCC Compliance Statement 381

E.2 Important Safety Instructions 381

E.3 IntraCare Warranty Statement 382

Appendix F. Online Warranty Registration 383

Chapter 1: Introduction

This switch provides a broad range of features for Layer 2 switching. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. You can also configure the switch to maximize the network performance.

Feature	Description
Configuration Backup and Restore	Backup to TFTP server
Authentication	Console, Telnet, web – User name / password, RADIUS, TACACS+ Web – HTTPS; Telnet – SSH SNMP – Community strings, IP address filtering Port – IEEE 802.1x, MAC address filtering
Access Control Lists	Supports up to 32 IP or MAC ACLs
DHCP Client	Supported
DHCP Server	Supported
Port Configuration	Speed, duplex mode and flow control
Rate Limiting	Input and output rate limiting per port
Port Mirroring	One or more ports mirrored to single analysis port
Port Trunking	Supports up to 6 trunks using either static or dynamic trunking (LACP)
Broadcast Storm Control	Supported
Static Address	Up to 16K MAC addresses in the forwarding table
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Protocol	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP)
Virtual LANs	Up to 255 using IEEE 802.1Q, port-based, protocol-based, or private VLANs
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP), and TCP/UDP Port
IP Routing	Routing Information Protocol (RIP), Open Shortest Path First (OSPF), static routes
ARP	Static and dynamic address configuration, proxy ARP
Multicast Filtering	Supports IGMP snooping and query
Multicast Routing	Supports DVMRP and PIM-DM

1.1 Description of Software Features

The switch provides a wide range of advanced performance enhancing features. Some of the management features are briefly described below.

Configuration Backup and Restore – Save the current configuration settings to a file on a TFTP server, and later download this file to restore the switch configuration settings.

Authentication – Permit management access through the console port, Telnet or web browser. User names and passwords are configured locally or verified through a remote authentication server (RADIUS or TACACS+). Port-based authentication is supported using the IEEE 802.1x protocol. This protocol uses the Extensible Authentication Protocol over LANs (EAPOL) to request a user name and password from the 802.1x client, and then verifies the client's right to access the network.

Other authentication options include HTTPS for secure management access through the web, SSH for secure management access over a Telnet-equivalent connection, IP address filtering for SNMP/web/Telnet management access, and MAC address filtering for port access.

Access Control Lists – Provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). Use ACLs to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

Port Configuration – Configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Full-duplex mode doubles the throughput of switch connections. Flow control manages network traffic during periods of congestion to prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard.

Rate Limiting – Control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Port Mirroring – Mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Port Trunking – Combine ports into an aggregate connection. Trunks can be manually set up or dynamically configured using IEEE 802.3ad Link Aggregation Control Protocol (LACP). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 6 trunks.

Broadcast Storm Control – Prevent broadcast traffic from overwhelming the network by managing the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it is suppressed until it reaches the defined level.

Static Addresses – Increase network security by restricting access for a known host to a specific port. A static address is assigned to a specific interface on this switch and are not moved. When a static address is detected by another interface, the address is ignored and is not written to the address table.

IEEE 802.1D Bridge –Facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 16K addresses. The switch supports IEEE 802.1D transparent bridging.

Store-and-Forward Switching – Copy each frame into memory before forwarding to another port. This ensures that all frames are a standard Ethernet size and are verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting port bandwidth.

To avoid dropping frames on congested ports, the switch provides 1 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

Spanning Tree Protocol – The switch supports these spanning tree protocols:

Spanning Tree Protocol (STP, IEEE 802.1D) – Adds a level of fault tolerance by allowing two or more redundant connections to be created between a pair of LAN segments. For multiple physical paths between segments, this protocol chooses a single path and disables others to ensure that only one route exists

between any two stations on the network, preventing the creation of loops. If the path should fail, an alternate path is activated to maintain the connection.

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – Reduce the convergence time for network topology changes to about 10% required by the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) –Provide an independent spanning tree for different VLANs. It simplifies network management, provides for faster convergence than RSTP. It limits the size of each region, and prevents VLAN members from being segmented from the group (as sometimes occurs with IEEE 802.1D STP). This protocol is direct extension of RSTP.

Virtual LANs – Provide support for up to 255 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned using GVRP. You can also manually assigned a port to a specific set of VLANs allowing the switch to restrict traffic to the VLAN groups where a user is assigned. By segmenting your network into VLANs, you can:

Eliminate broadcast storms that severely degrade performance in a flat network.

Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.

Provide data security by restricting all traffic to the originating VLAN.

Restrict private VLANs to restrict traffic to pass only between data ports and uplink ports. This isolates adjacent ports within the same VLAN, and allows you to limit the number of VLANs needing configuration.

Restrict traffic to specified interfaces based on protocol type.

Traffic Prioritization – Prioritize each packet based on the required level of service, using eight priority queues with strict or Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. Use these functions to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic is prioritized based on the priority bits in the IP frame’s Type of Service (ToS) octet or the number of the TCP/UDP port. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Multicast Filtering – Assign specific multicast traffic to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration.

1.2 System Defaults

The system defaults are in the configuration file “Factory_Default_Config.cfg.” Set this files as the startup configuration file to resent the defaults (see, **2.9.1 Downloading Configuration Settings from a Server**).

The following table lists some of the basic system defaults.

Function	Parameter	Default
Console Port Connection	Baud Rate	Auto
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication	Privileged Exec Level	Username “root” Password “Asante”
	Normal Exec Level	Username “root” Password “Asante”
	Enable Privileged Exec from Normal Exec Level	Password “super”
	RADIUS Authentication	Disabled
	S/TATACS/TATACS Authentication	Disabled
	802.1x Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443
SNMP	Community Strings	“public” (read only) “private” (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled

Port Configuration	Admin Status Auto-negotiation Flow Control Port Capability	Enabled Enabled Disabled **1000BASE-T** – 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled **1000BASE-SX/LX/LH** – 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled
Rate Limiting	Input and Output Limits	Disabled
Port Trucking	Static Trucks LACP (all ports)	None Disabled
Broadcast Storm Protection	Status Broadcast Limit Rate	Enabled (all ports) 500 packets per second
Spanning Tree Protocol	Status Fast Forwarding (edge port)	Enabled, MSTP (Defaults: All values based on IEEE 802.1s) Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN PVID Acceptable Frame Type Ingress Filtering Switchport Mode (egress mode) GVRP (global) GVRP (port interface)	1 1 All Disabled Hybrid: tagged/untagged frames Disabled Disabled

Traffic Prioritization	Ingress Port Priority	0
	Weighted Round Robin	Queue: 0 1 2 3 4 5 6 7 Weight: 2 0 1 3 4 5 6 7
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled
IP Settings	IP Address	192.168.0.1
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP	Client: Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes Proxy Disabled
	RIP	Disabled
	OSPF	Disabled
	Port Security	Learning is enabled
DNS Server	Lookup	Disabled
Multicast Filtering	IGMP Snooping	Snooping: Enabled Querier: Enabled
	IGMP (Layer 3)	Disabled
Multicast Routing	DVMRP	Disabled
	PIM-DIM	Disabled
System Log	Status	Enabled
	Messages Logged	Levels 0-37 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Disabled
SNTP	Clock Synchronization	Disabled

Chapter 2: Initial Configuration

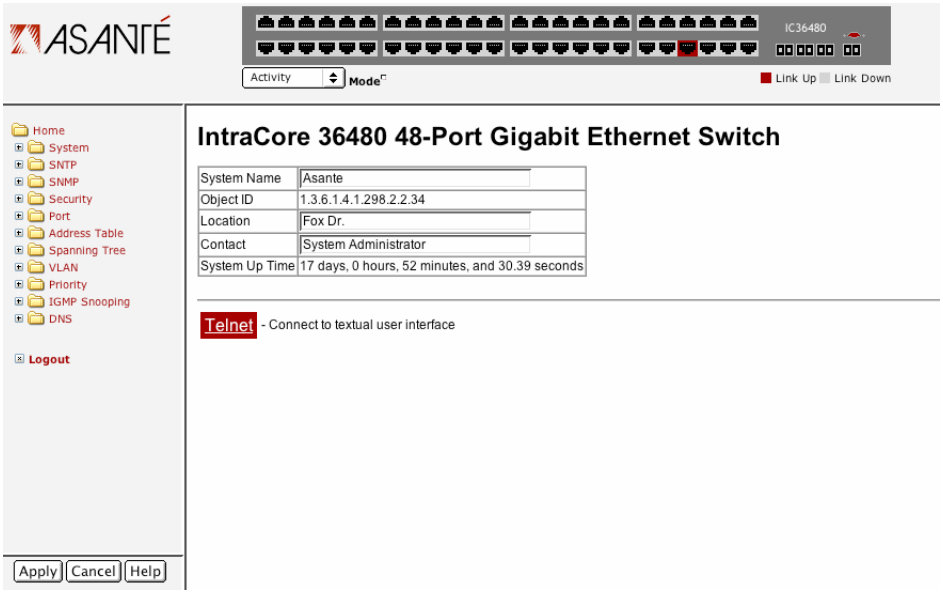
2.1 Connecting to the Switch

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a web-based interface. You can connect a PC directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: The IP address for this switch is 192.168.0.1. To change this address, refer to **Section 2.4 Setting an IP Address.**

The switch's HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. Access the switch's web management interface from any computer attached to the network.

The following illustration shows the web interface.



Access the CLI program with a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch's management agent also supports SNMP (Simple Network Management Protocol). Manage this switch using the SNMP agent from any system in the network using network management software such as HP OpenView.

The switch's web interface, CLI configuration program, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords for up to 16 users
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port

- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by limiting input or output rates
- Control port access through IEEE 802.1x security or static address filtering
- Filter packets using Access Control Lists (ACLs)
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IGMP multicast filtering
- Upload and download system firmware using TFTP
- Upload and download switch configuration files using TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to 6 static or LACP trunks
- Enable port mirroring
- Set broadcast storm control on any port
- Display system information and statistics

2.2 Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. The switch comes with a null-modem console cable.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
    - Select the appropriate serial port (COM port 1 or COM port 2).
    - Set to 9600 baud rate if you want to view all the system initialization messages.
    - Set the data format to 8 data bits, 1 stop bit, and no parity.
    - Set flow control to none.
    - Set the emulation mode to VT100.

4. When using HyperTerminal, select Terminal keys, not Windows keys.

When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

Refer to section **15.1 Line Commands** for a complete description of console configuration options.

The console login screen appears when the system is setup correctly.

For a description of how to use the CLI, see **Chapter 14: Using the Command Line Interface**. For a list of all the CLI commands and detailed information on using the CLI, refer to section **14.5.3 Command Groups**.

2.2.1 Console Connections

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels is controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press **<Enter>**. The "User Access Verification" procedure starts.

2. At the Username prompt, enter "root."

3. At the Password prompt, also enter "Asante." (The password characters are not displayed on the console screen.)

4. The session is opened and the CLI displays the "Console#" prompt indicating you have access at the Privileged Exec level.

2.2.3 Remote Connections

Before accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

This switch supports four concurrent Telnet/SSH sessions.

2.3 Setting a Password

If this is your first time logging in to the switch, the following login information is the standard default:

[Default IP Address: 192.168.0.1]
[Default username: root]
[Default password: Asante]

You should define new usernames and passwords using the "**username**" command.

Passwords can consist of up to eight alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface and type the default user name **root** and password **Asante** to access the Privileged Exec level.

2. Type **configure** and press **Enter**.

3. Type **username guest password *0 [password]*** where *password* is your new password. Press **Enter**.

```
Switch> enable
Password: <no password by default; press Enter>
Switch# configure
Switch(config)#username admin password 0 [password ]
Switch(config)# admin Password

Switch(config)# exit
```

2.4 Setting an IP Address

This section describes how to configure an IP interface for management access over the network.

Note: By default, DHCP provides the IP address for the switch.

To manually configure an address, you need to change the switch's default settings (IP address 192.168.0.1 and netmask 255.255.255.0) to values that are compatible with your network. Establish a default gateway between the switch and management stations that exist on another network segment.

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

You must establish IP address information for the switch to obtain management access through the network. Do this in either of the two following ways:

Manual — Input the IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you also need to specify the default gateway.

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Command Attributes

Management VLAN – ID of the configured VLAN (1-4094, no leading zeroes). By default, all ports on the switch are members of VLAN 1. You can attach the management station to a port belonging to any VLAN, when the VLAN has an IP address.

IP Address Mode – Specifies how IP functionality is enabled, by manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP does not function until the server replies. Periodically, the switch sends broadcast requests for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)

IP Address – Address of the VLAN interface allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 192.168.0.1)

Subnet Mask – Mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)

Gateway IP Address – IP address of the gateway router between this device and management stations that exist on other network segments. (Default: 0.0.0.0)

MAC Address – The physical layer address for this switch.

2.4.1 Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

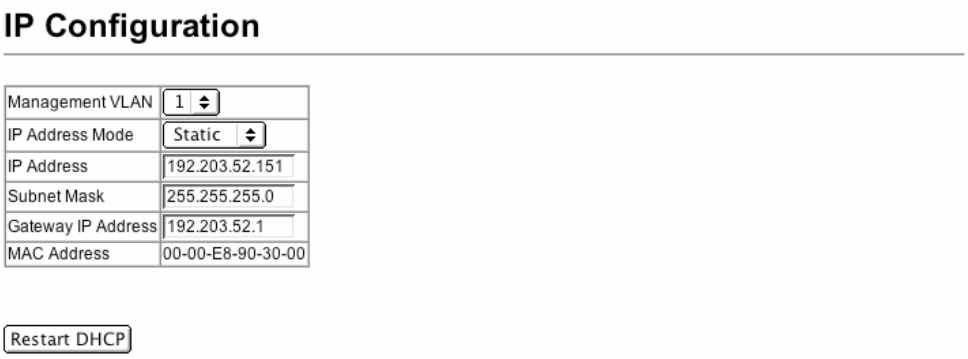
- IP address for the switch
- Default gateway for the network
- Network mask for this network

To assign an IP address to the switch, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode and press **Enter**.
2. Type “ip address *ip-address netmask*,” where “ip-address” is the switch IP address and “netmask” is the network mask for the network and press **Enter**.
3. Type “exit” to return to the global configuration mode prompt and press **Enter**.
4. To set the IP address of the default gateway for the network to which the switch belongs, type “ip default-gateway *gateway*,” where “gateway” is the IP address of the default gateway and press **Enter**.

Web

Click System – IP Configuration. Select the VLAN through which the management station is attached, set the IP Address Mode to “Static,” enter the IP address, subnet mask and gateway, then click Apply.



CLI

Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

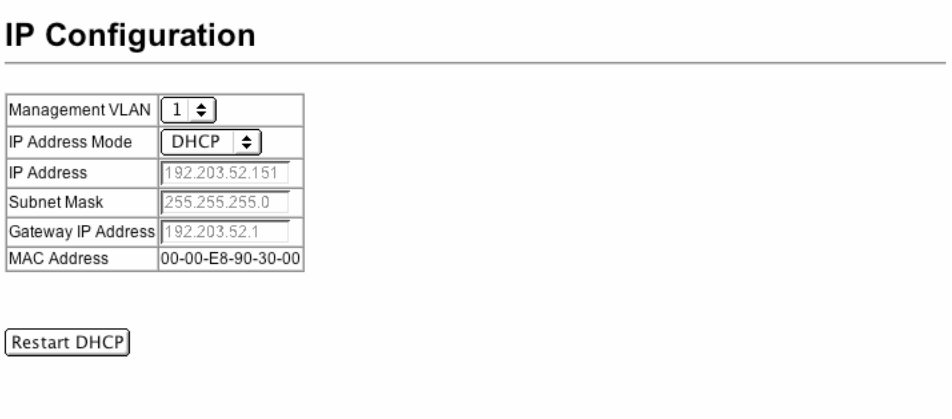
2.4.2 Dynamic Configuration

You can set the switch for dynamic configuration when your network provides DHCP/BOOTP services. If you select the “bootp” or “dhcp” option, IP is active but does not function until a BOOTP or DHCP reply is received. You need to use the **ip dhcp restart** command to start broadcasting service requests. To obtain IP configuration information, the switch periodically sends requests. BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.

When you save “bootp” or “dhcp” to the startup-configuration file, broadcast service requests are sent at launch.

Web

Click System – IP Configuration. Specify the VLAN where the management station is attached, set the IP Address Mode to DHCP or BOOTP. Click Apply to save your changes. Then click Restart DHCP to immediately request a new address. Note that the switch will also broadcast a request for IP configuration settings on each power reset.



Note: If you lose your management connection, use a console connection and enter “show ip interface” to determine the new switch address.

CLI

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type **interface vlan 1** to access the interface-configuration mode. Press **Enter**.

2. At the interface-configuration mode prompt, use one of the commands in the following table:

Command	Purpose
ip address dhcp	Obtains IP settings using DHCP
ip address bootp	Obtains IP settings using BOOTP
ip dhcp restart client	Starts broadcasting service requests

3. Wait a few minutes, and then check the IP configuration settings by typing **show ip interface** and press **Enter**.

4. Then save your configuration changes by typing “copy running-config startup-config.” Enter the startup file name and press **Enter.**

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

2.5 Enabling SNMP Management Access

You can configure the switch to accept management commands from Simple Network Management Protocol (SNMP) applications such as HP OpenView. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. You can also configure the switch to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

2.5.1 Community Strings

Community strings are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users or user groups, and set the access level.

The default strings are:

public - with read-only access. Authorized management stations are only able to retrieve MIB objects.

private - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note: If you do not intend to utilize SNMP, delete both of the default community strings. If there are no community strings, then SNMP management access to the switch is disabled.

To prevent unauthorized access to the switch using SNMP, change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>. (Default: read only)

2. To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw
```

```
Console(config)#snmp-server community private
Console(config)#
```

2.5.2 Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch.

To configure a trap receiver, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server host *host-address community-string*,” where “host-address” is the IP address for the trap receiver and “community-string” is the string associated with that host and press **Enter**.

2. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server enable traps command. Type “snmp-server enable traps *type*,” where “type” is either **authentication** or **link-up-down** and press **Enter**.

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

2.6 Saving Configuration Settings

Configuration commands only modify the running configuration file and are lost when you reboot the switch. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the “copy” command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type “copy running-config startup-config” and press **Enter**.

2. Enter the name of the start-up file and press **Enter**.

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

2.7 Managing System Files

The switch’s flash memory supports three types of system files that can be managed by the CLI program, web interface, or SNMP. The switch’s file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The three types of files are:

Configuration — This file stores system configuration information and is created when configuration settings are saved. Saved configuration files can be used as a system start-up file or uploaded through TFTP to a server for backup. A file named “Factory_Default_Config.cfg” contains all the system default settings. You cannot delete this file from the system. For more information, see Section 2.9 Saving or Restoring Configuration Settings.

Operation Code — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces. See Section 2.8 Managing Firmware for more information.

Diagnostic Code — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Due to the size limit of the flash memory, the switch supports only two operation code files. You can have as many diagnostic code files and configuration files as available flash memory space allows.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note: Download configuration files using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, when the system reboots, the settings need to be copied from the running-config to a permanent file.

2.8 Managing Firmware

You can upload/download firmware to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version.

Command Attributes

TFTP Server IP Address – The IP address of a TFTP server.

File Name – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

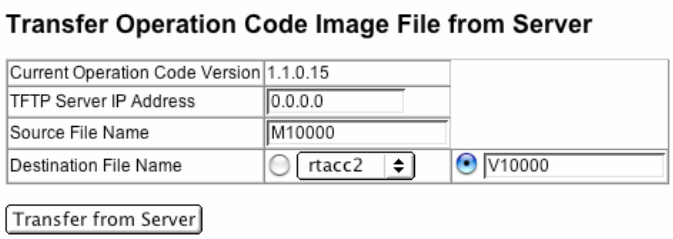
Note: Up to two copies of the system software (For example, the runtime firmware) can be stored in the file directory on the switch. You cannot delete the current startup version of this file.

2.8.1 Downloading System Software from a Server

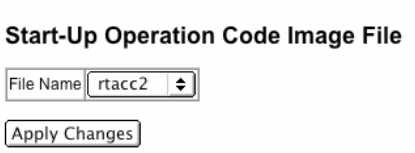
When downloading runtime code, you can specify the destination file name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

Web

Click System – File, Firmware. Enter the IP address of the TFTP server, enter the file name of the software to download, select a file on the switch to overwrite or specify a new file name, then click Transfer from Server. To start the new firmware, reboot the system via the System/Reset menu.



If you download to a new destination file, then select the file from the drop-down box for the operation code used at startup, and click Apply Changes. To start the new firmware, reboot the system via the System/Reset menu.



CLI

Enter the IP address of the TFTP server, select “config” or “opcode” file type, then enter the source and destination file names, set the new file to start up the system, and then restart the switch.

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: M100000.bix
Destination file name: V1.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode:V1.0
Console(config)#exit
Console#reload
```

2.9 Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server. Use this file to restore settings.

Command Attributes

TFTP Server IP Address – The IP address of a TFTP server.

File Name — The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

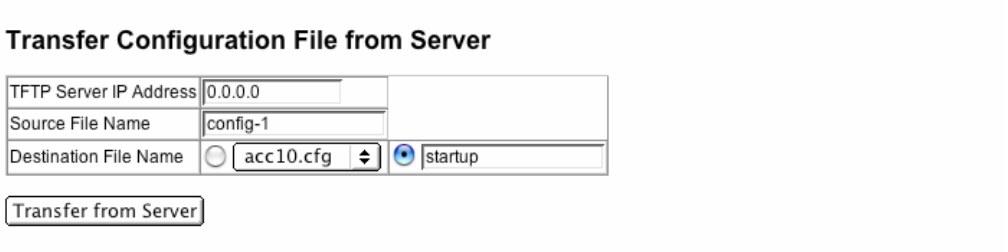
Note: The available flash memory space limits the maximum number of user-defined configuration files.

2.9.1 Downloading Configuration Settings from a Server

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. The file “Factory_Default_Config.cfg” can be copied to the TFTP server, but cannot be used as the destination on the switch.

Web

Click System – File, Configuration. Enter the IP address of the TFTP server, enter the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click Transfer from Server.



If you download to a new file name, then select the new file from the drop-down box for Startup Configuration File, and press Apply Changes. To use the new settings, reboot the system via the System/Reset menu.

CLI

Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config
TFTP server ip address: 192.168.1.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
```

If you download the startup configuration file under a new file name, you can set this file as the startup file later, and then restart the switch.

```
Console#config
Console(config)#boot system config: startup-new
Console(config)#exit
Console#reload
```

2.9.2 Resetting the System

Web

Click System – Reset. Click the Reset button to restart the switch.

CLI

Use the reload command to restart the switch.

```
Console#reload
System will be restarted, continue <y/n>?
```

Note: When restarting the system, it will always run the Power-On Self-Test.

2.9.3 Renewing DCHP

DHCP may lease addresses to clients indefinitely or for a specific period. If the address expires or the switch is moved to another network segment, you lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service through the CLI.

Web

If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

CLI

Enter the following command to restart DHCP service.

```
Console#ip dhcp restart
Console#
```

2.10 Basic Management

The section describes setting the system clock, displaying system information, displaying hardware and software versions and bridge expansion capabilities.

2.10.1 Setting the System Clock

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a timeserver (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock using the CLI. (Refer to the **calendar set** command in Chapter 16.) If the clock is not set, the switch only records the time from the factory default set at the last bootup.

This switch acts as an SNTP client in two modes:

Unicast – The switch periodically sends a request for a time update to a configured timeserver. You can configure up to three timeserver IP addresses. The switch will attempt to poll each server in the configured sequence.

Broadcast – The switch sets its clock from a timeserver in the same subnet that broadcasts time updates. If there is more than one SNTP server, the switch accepts the first broadcast it detects and ignores broadcasts from other servers.

2.10.2 Displaying System Information

You can easily identify the system by displaying the device name, location and contact information.

Field Attributes

System Name: Name assigned to the switch system.

Object ID: MIB II object ID for switch's network management subsystem.

Location – Specifies the system location.

Contact: Administrator responsible for the system.

System Up Time: Length of time the management agent has been running.

These additional parameters are displayed for the CLI.

MAC Address: The physical layer address for this switch.

Web server: Shows if management access using HTTP is active.

Web server port: Shows the TCP port number used by the web interface.

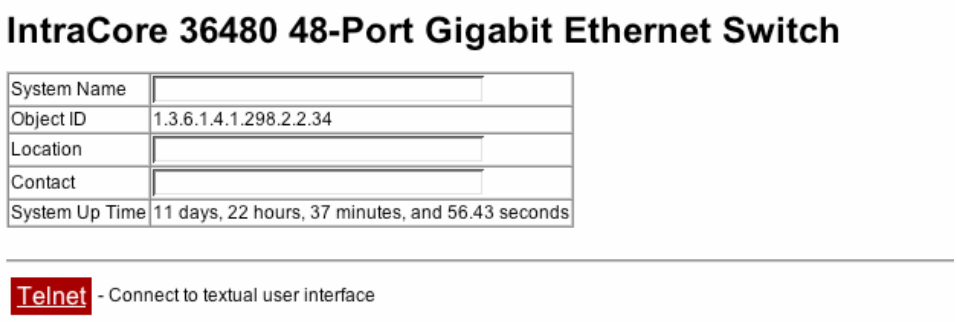
Web secure server: Shows if management access through HTTPS is active.

Web secure server port: Shows the TCP port used by the HTTPS interface.

POST result: Shows results of the power-on self-test

Web

Click System – System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows access to the Command Line Interface through a Telnet connection.)



CLI: Specify the hostname, location and contact information.

```
Console(config)#hostname R&D 5
Console(config)#snmp-server location WC
Console(config)#snmp-server contact james
Console(config)#exit
Console#show system
System description: 44 10/100/1000 ports + 4 Gigabit Combo ports L2/L4 managed
standalone switch
System OID string: 1.3.6.1.4.1.259.6.10.51
```

```
System information
 System Up time: 0 days, 2 hours, 4 minutes, and 7.13 seconds
 System Name            : R&D 5
 System Location        : WC 9
 System Contact         : James
 MAC address            : 00-30-f1-47-58-3a
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result
DUMMY Test 1.................PASS
UART LOOP BACK Test..........PASS
DRAM Test....................PASS
Timer Test...................PASS
PCI Device 1 Test............PASS
Switch Int Loopback test.....PASS
Crossbar Int Loopback Test...PASS

Done All Pass.
Console#
```

2.10.3 Displaying Switch Hardware/Software Versions

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Field Attributes

Main Board

Serial Number: The serial number of the switch.

Number of Ports: Number of built-in RJ-45 ports and SFP slots.

Hardware Version: Hardware version of the main board.

Internal Power Status: Displays the status of the internal power supply.

Redundant Power Status: (CLI only) Displays the status of the redundant power supply.

Management Software

Loader Version: Version number of loader code.

Boot-ROM Version: Version of Power-On Self-Test (POST) and boot code.

Operation Code Version: Version number of runtime code.

Role: Shows that this switch is operating as Master (For example, operating stand-alone).

Web

Click System – Switch Information.

Switch Information

Main Board:

Serial Number	
Number of Ports	48
Hardware Version	
Internal Power Status	Active

Management Software:

Loader Version	2.0.0.1
Boot-ROM Version	2.0.0.2
Operation Code Version	1.1.0.15
Role	Master

CLI

Use the following command to display version information.

```
Console#show version
Unit1
 Serial number           :A305051234
 Hardware version        :R0A
 Number of ports         :24
 Main power status       :up
 Redundant power status :not present
Agent(master)
 Unit id                 :1
 Loader version          :1.0.0.1
 Boot rom version        :1.0.0.1
 Operation code version :1.1.0.13
Console#
```

2.10.4 Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

Field Attributes

Extended Multicast Filtering Services: This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).

Traffic Classes: This switch provides mapping of user priorities to multiple traffic classes. (Refer to the section “Number of Egress Traffic Classes” under the section **11.1 Setting the Default Priority for Interfaces**.)

Static Entry Individual Port: This switch allows static filtering for unicast and multicast addresses. (Refer to **8.1 Setting Static Addresses** section.)

VLAN Learning: This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.

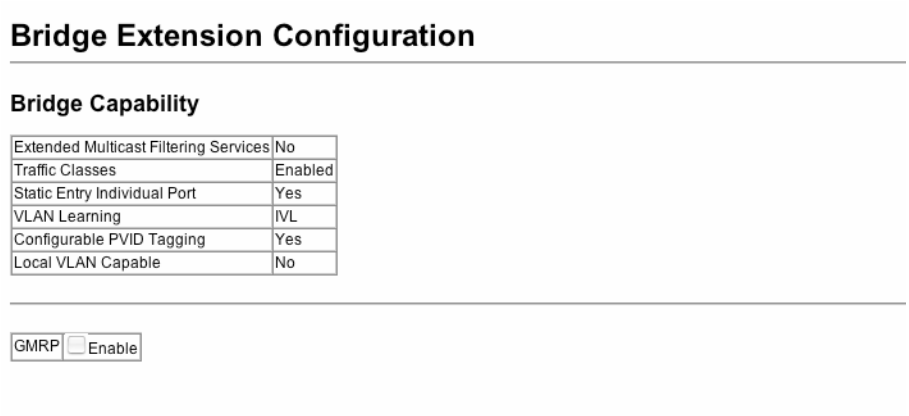
Configurable PVID Tagging: This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to **Chapter 10 Configuring VLANs**.)

Local VLAN Capable: This switch supports multiple local bridges; For example, multiple spanning trees. (Refer to section **3.3 Configuring Multiple Spanning Trees**.)

GMRP: GARP Multicast Registration Protocol (GMRP) allows network devices to register end stations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Web

Click System – Bridge Extension.



CLI

Enter the following command.

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Disabled
 GMRP: Disabled
Console#
```

Chapter 3: Configuring Global Settings

The switch's HTTP web agent allows you to configure switch parameters, monitor port connections and display statistics using a standard web browser such as Internet Explorer 5, Netscape 6, Apple Safari 1.2, Mozilla Firefox 0.8 or later, using Windows Me/2000/XP, Mac OS X 10.3 or Linex. The recommended screen resolution is 1024 x 768 or higher. You can access the switch's web management interface from any computer attached to the network.

Note: The screen captures used in this manual are based on the IC36480, but are all the same for the IC36240 except for the port count.

Before accessing the switch from a web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See **Section 2.4 Setting an IP Address**.)

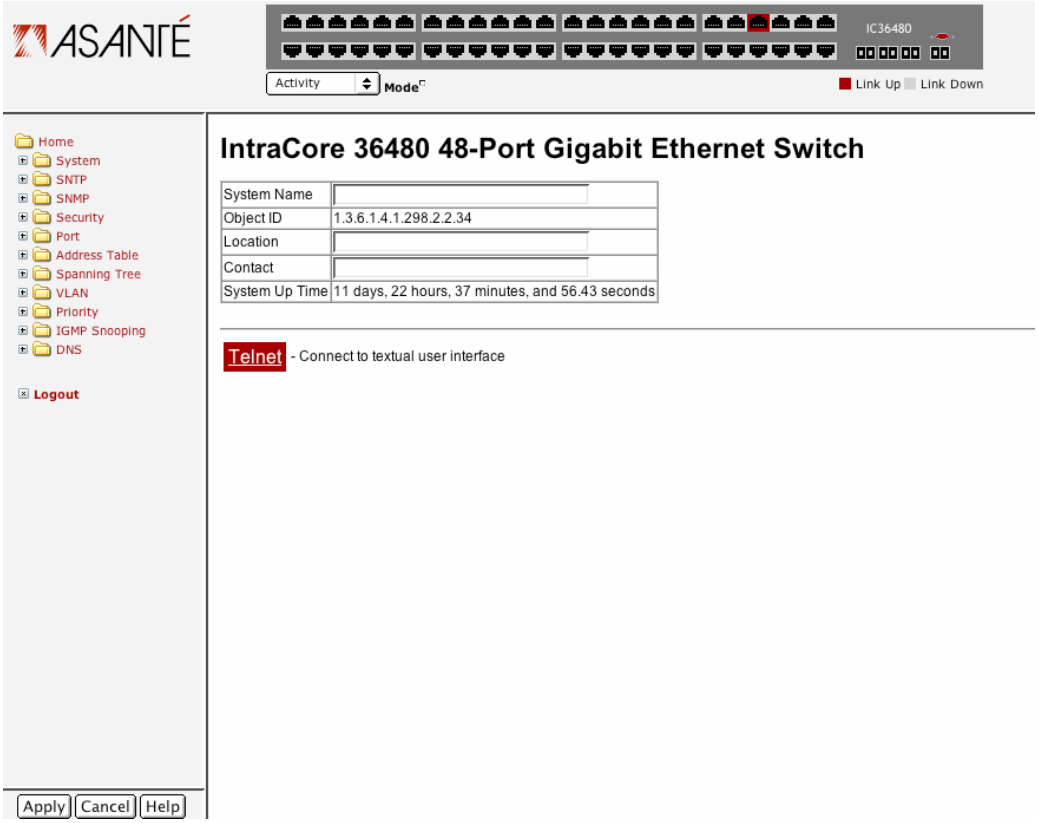
2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See **Section 2.3 Setting a Password** in chapter 2.)

3. After you enter a user name and password, you will have access to the system configuration program.

Note: You are allowed three attempts to enter the correct password; after the third attempt, the current connection is terminated.

If you log into the web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as "admin" (Privileged Exec level), you can change the settings on any page.

When you manage the switch using the web interface the home page, as shown below, provides the main menu on the left side of the screen and the screen information on the right.



You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to **Appendix A: Web and Command Line Interface Overview**.

3.1 Configuring Spanning Tree

The follow section describe using and configuring spanning tree protocols including rapid spanning tree (RSTP) and multiple spanning trees (MSTP).

3.1.1 Spanning Tree Global Settings

Global settings apply to the entire switch.

Spanning Tree Protocol

Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network.

Rapid Spanning Tree Protocol

RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

STP Mode – If the switch receives an 802.1D BPDU (For example, STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Multiple Spanning Tree Protocol

To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

- A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
- Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

3.1.2 Spanning Tree Basic Configuration

This section describes the basic configuration for STP, including the global settings and root device configuration,

Global Settings

Spanning Tree State – Enables/disables STA on this switch. (Default: Enabled)

Spanning Tree Type – Specifies the type of spanning tree used on this switch:

- STP: Spanning Tree Protocol (IEEE 802.1D); For example, when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
- RSTP: Rapid Spanning Tree (IEEE 802.1w)
- MSTP: Multiple Spanning Tree (IEEE 802.1s); MSTP is the default.

Priority – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)

- Default: 32768
- Range: 0-61440, in steps of 4096
- Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Root Device Configuration

Hello Time – Interval (in seconds) at which the root device transmits a configuration message.

- Default: 2
- Minimum: 1
- Maximum: The lower of 10 or [(Max. Message Age / 2) -1]

Maximum Age – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)

- Default: 20
- Minimum: The higher of 6 or [2 x (Hello Time + 1)].
- Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

Forward Delay – The maximum time (in seconds) this device will wait before changing states (For example, discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

- Default: 15
- Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
- Maximum: 30

3.1.3 Configuration Settings for RSTP

The following attributes apply to both RSTP and MSTP:

Path Cost Method – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

- Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
- Short: Specifies 16-bit based values that range from 1-65535.

Transmission Limit – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

3.1.4 Configuration Settings for MSTP

The following configuration settings apply to the MSTP.

Max Instance Numbers – The maximum number of MSTP instances to which this switch can be assigned. (Default: 65)

Region Revision* – The revision for this MSTI. (Range: 0-65535; Default: 0)

Region Name* – The name for this MSTI. (Maximum length: 32 characters)

Maximum Hop Count – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

Note: The MST name and revision number are both required to uniquely identify an MST region.

Configuring Switch Using the Web or CLI

Web

Click Spanning Tree – STA, Configuration. Modify the required attributes, and click Apply.

MSTP Configuration:

Max Instance Numbers	64
Configuration Digest	0xAC36177F50283CD4B83821D8AB26DE62
Region Revision (0-65535)	0
Region Name	00 00 e8 90 30 00
Max Hop Count (1-40)	20

CLI

This example enables Spanning Tree Protocol, sets the mode to MST, and then configures the STA and MSTP parameters.

```
Console(config)#spanning-tree
Console(config)#spanning-tree mode mstp
Console(config)#spanning-tree priority 45056
Console(config)#spanning-tree hello-time 5
Console(config)#spanning-tree max-age 14
Console(config)#spanning-tree forward-time 20
Console(config)#spanning-tree pathcost method long
Console(config)#spanning-tree transmission-limit 4
Console(config)#spanning-tree mst configuration
Console(config-mstp)#revision 1
Console(config-mstp)#name R&D
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

3.1.5 Displaying Interface Settings

The STA Port Information and STA Trunk Information pages display the status of ports and trunks in the Spanning Tree.

Field Attributes

Spanning Tree – Shows if STA has been enabled on this interface.

STA Status – Displays current state of this port within the Spanning Tree:

Discarding–Port receives STA configuration messages, but does not forward packets.

Learning–Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.

Forwarding–Port forwards packets, and continues learning addresses.

The rules defining port status are:

- A port on a network segment with no other STA compliant bridging device is always forwarding.
- If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
- All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.

Forward Transitions – The number of times this port has transitioned from the Learning state to the Forwarding state.

Designated Cost – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.

Designated Bridge – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.

Designated Port – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.

Oper Link Type – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration in section **3.2 Configuring Interface Settings**.

Oper Edge Port – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration in section **3.2 Configuring Interface Settings** (for example, true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.

Port Role – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (for example, root port), connecting a LAN through the bridge to the root bridge (for example, designated port), or is the MSTI regional root (for example, master port). The are also assigned as an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (For example, disabled port) if a port has no role within the spanning tree.

Trunk Member – Indicates if a port is a member of a trunk. (STA Port Information only)

These additional parameters are only displayed for the CLI:

Admin status – Shows if this interface is enabled.

External path cost – The path cost for the IST. This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)

Internal path cost – The path cost for the MST. Refer to the proceeding item “External Path Cost” for more information.

Priority – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (For example, lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.

Designated root – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.

Fast forwarding – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.

Admin Edge Port – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning

tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. The Edge Port should only be enabled for ports connected to an end-node device.

Admin Link Type – The link type attached to this interface.

Point-to-Point – A connection to exactly one other bridge.

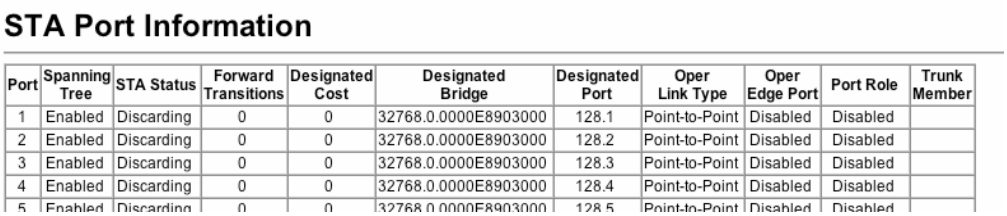
Shared – A connection to two or more bridges.

Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.

Configuring Switch Using the Web or CLI

Web

Click Spanning Tree – STA, Port Information or Trunk Information.



STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Discarding	0	0	32768.0.0000E8903000	128.1	Point-to-Point	Disabled	Disabled	
2	Enabled	Discarding	0	0	32768.0.0000E8903000	128.2	Point-to-Point	Disabled	Disabled	
3	Enabled	Discarding	0	0	32768.0.0000E8903000	128.3	Point-to-Point	Disabled	Disabled	
4	Enabled	Discarding	0	0	32768.0.0000E8903000	128.4	Point-to-Point	Disabled	Disabled	
5	Enabled	Discarding	0	0	32768.0.0000E8903000	128.5	Point-to-Point	Disabled	Disabled	

CLI

This example shows the STA attributes for port 5.

```
Console#show spanning-tree ethernet 1/5
Eth  1/ 5 information
---------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 External path cost   : 10000
 Internal path cost   : 10000
 Priority             : 128
 Designated cost      : 200000
 Designated port      : 128.5
 Designated root      : 61440.0.0000E9313131
 Designated bridge    : 61440.0.0000E9313131
 Fast forwarding      : enable
 Forward transitions  : 0
 Admin edge port      : enable
 Oper edge port       : enable
 Admin Link type      : auto
 Oper Link type       : point-to-point
 Spanning Tree Status : enable

Console#
```

3.2 Configuring Interface Settings

You can configure RSTP and MSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate

the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding.

3.2.1 Attributes

Read-Only Attributes

STA State – Displays current state of this port within the Spanning Tree. (For more information, refer to section **3.1.5 Displaying Interface Settings**.)

- Discarding - Port receives STA configuration messages, but does not forward packets.
- Learning - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
- Forwarding - Port forwards packets, and continues learning addresses.

Trunk – Indicates if a port is a member of a trunk. (STA Port Configuration only)

Configuration Attributes

Spanning Tree – Enables/disables STA on this interface. (Default: Enabled).

Priority – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (For example, lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier is enabled.

- Default: 128
- Range: 0-240, in steps of 16

Path Cost – This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (see section **9.9.1)**, the maximum path cost is 65,535.

Range :

- Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

Default:

- Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000

Admin Link Type – The link type attached to this interface.

Point-to-Point – A connection to exactly one other bridge.

Shared – A connection to two or more bridges.

Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)

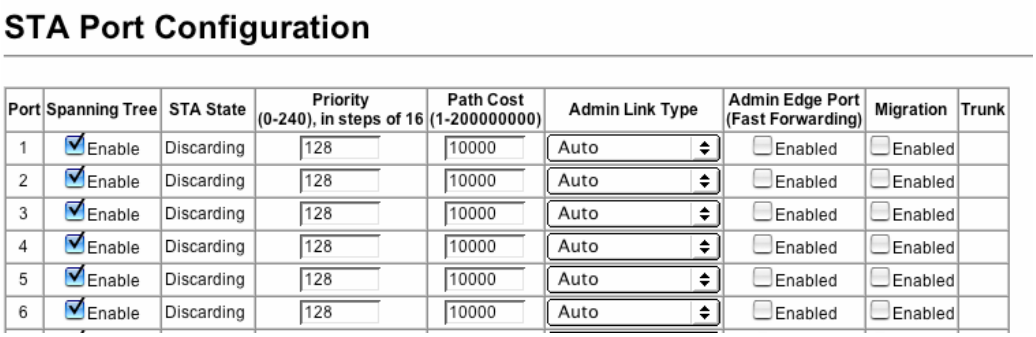
Admin Edge Port (Fast Forwarding) – Enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. The Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)

Migration – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. You can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

Configuring Switch Using the Web or CLI

Web

Click Spanning Tree – STA, Port Configuration or Trunk Configuration. Modify the required attributes, then click Apply.


STA Port Configuration
Port
Spanning Tree
STA State
Priority (0-240), in steps of 16
Path Cost (1-200000000)
Admin Link Type
Admin Edge Port (Fast Forwarding)
Migration
Trunk
1 Enable Discarding 128 10000 Auto Enabled Enabled
2 Enable Discarding 128 10000 Auto Enabled Enabled
3 Enable Discarding 128 10000 Auto Enabled Enabled
4 Enable Discarding 128 10000 Auto Enabled Enabled
5 Enable Discarding 128 10000 Auto Enabled Enabled
6 Enable Discarding 128 10000 Auto Enabled Enabled

CLI

This example sets STA attributes for port 7.

```
Console(config)#interface ethernet 1/7
Console(config-if)#no spanning-tree spanning-disabled
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#spanning-tree cost 5
Console(config-if)#spanning-tree link-type auto
Console(config-if)#no spanning-tree edge-port
Console(config-if)#
```

3.3 Configuring Multiple Spanning Trees

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default, all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 65 instances. You should try to group VLANs that cover the same general area of your network. You must configure all bridges within the same MSTI

Region (section **3.1.1**) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

To use multiple spanning trees:

1. Set the spanning tree type to MSTP (STA Configuration, section **3.1.1**).

2. Enter the spanning tree priority for the selected MST instance (MSTP VLAN Configuration).

3. Add the VLANs that will share this MSTI (MSTP VLAN Configuration).

Note: All VLANs are automatically added to the IST (Instance 0).

To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

3.3.1 Attributes

MST Instance – Instance identifier of this spanning tree. (Default: 0)

Priority – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)

VLANs in MST Instance – VLANs assigned this instance.

MST ID – Instance identifier to configure. (Range: 0-4094; Default: 0)

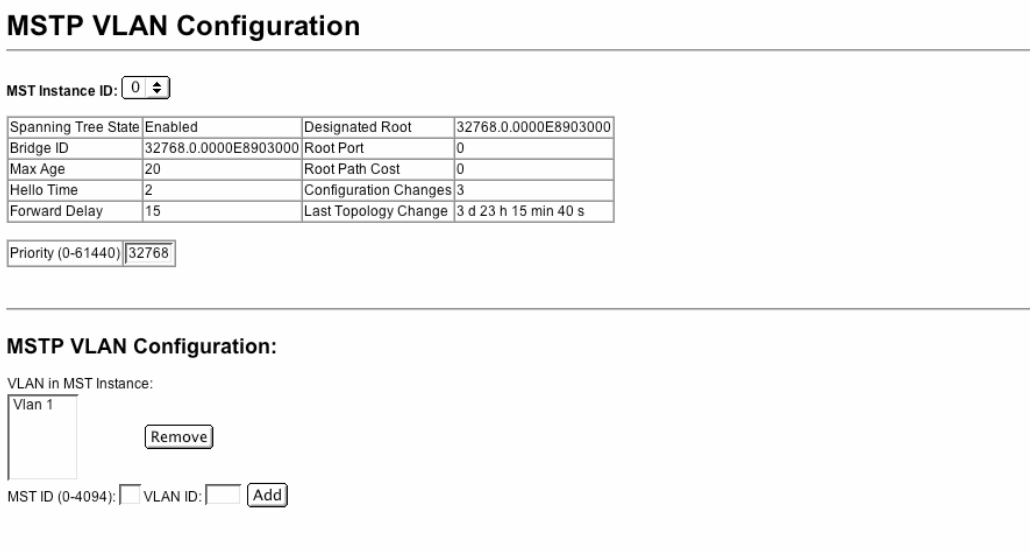
VLAN ID – VLAN to assign to this selected MST instance. (Range: 1-4094)

The other global attributes are described under section **9.1.1 Displaying Global Settings**. The attributes displayed by the CLI for individual interfaces are described under section **3.1.5 Displaying Interface Settings**.

Configuring Switch Using the Web or CLI

Web

Click Spanning Tree – MSTP, VLAN Configuration. Select an instance identifier from the list, set the instance priority, and click Apply. To add the VLAN members to an MSTI instance, enter the instance identifier, the VLAN identifier, and click Add.


MSTP VLAN Configuration
MST Instance ID: 0
Spanning Tree State Enabled Designated Root 32768.0.0000E8903000
Bridge ID 32768.0.0000E8903000 Root Port 0
Max Age 20 Root Path Cost 0
Hello Time 2 Configuration Changes 3
Forward Delay 15 Last Topology Change 3 d 23 h 15 min 40 s
Priority (0-61440) 32768
MSTP VLAN Configuration:
VLAN in MST Instance:
Vlan 1
Remove
MST ID (0-4094): VLAN ID: Add

CLI

This displays STA settings for instance 1, followed by settings for each port.

```
Console#show spanning-tree mst 1
Spanning-tree information
---------------------------------------------------------------------
 Spanning tree mode               :MSTP
 Spanning tree enable/disable     :enable
 Instance                         :1
 Vlans configuration              :1-5
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Max hops                         :20
 Remaining hops                   :20
 Designated Root                  :4096.2.0000E9313131
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :0
 Last topology changes time (sec.):646
 Transmission limit               :3
 Path Cost Method                 :long
---------------------------------------------------------------------
Eth  1/ 7 information
---------------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 External path cost   : 10000
 Internal path cost   : 10000
 Priority             : 128
 Designated cost      : 0
 Designated port      : 128.7
```

```
 Designated root      : 4096.2.0000E9313131
 Designated bridge    : 4096.2.0000E9313131
 Fast forwarding      : enable
 Forward transitions  : 0
 Admin edge port      : enable
 Oper edge port       : enable
 Admin Link type      : auto
 Oper Link type       : point-to-point
 Spanning Tree Status : enable
.
.
.
```

CLI

This example sets the priority for MSTI 1, and adds VLANs 1-5 to this MSTI.

```
Console(config)#spanning-tree mst configuration
Console(config-mst)#mst 1 priority 4096
Console(config-mstp)#mst 1 vlan 1-5
Console(config-mst)#
```

3.3.2 Displaying Interface Settings for MSTP

The MSTP Port Information and MSTP Trunk Information pages display the status of ports and trunks in the selected MST instance.

Field Attributes

MST Instance ID – Instance identifier to configure. (Range: 0-4094; Default: 0)

The other attributes are described under **Section 3.1.5 Displaying Interface Settings**.

Configuring Switch Using the Web or CLI

Web

Click Spanning Tree – MSTP, Port Information or Trunk Information. Select the required MST instance to display the current spanning tree values.

MSTP Port Information

MST Instance ID: 0

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Discarding	0	0	32768.0.0000E8903000	128.1	Point-to-Point	Disabled	Disabled	
2	Discarding	0	0	32768.0.0000E8903000	128.2	Point-to-Point	Disabled	Disabled	
3	Discarding	0	0	32768.0.0000E8903000	128.3	Point-to-Point	Disabled	Disabled	

CLI

This displays STA settings for instance 0, followed by settings for each port. The settings for instance 0 are global settings that apply to the IST (section **9.1.1**), the settings for other instances only apply to the local spanning tree.

```
Console#show spanning-tree mst 0
Spanning-tree information
----------------------------------------------------------------
 Spanning tree mode               :MSTP
 Spanning tree enable/disable     :enable
 Instance                         :0
 Vlans configuration              :1-4094
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Max hops                         :20
 Remaining hops                   :20
 Designated Root                  :32768.0.0000ABCD0000
 Current root port                :1
 Current root cost                :200000
 Number of topology changes       :1
 Last topology changes time (sec.):645
 Transmission limit               :3
 Path Cost Method                 :long
----------------------------------------------------------------
Eth  1/ 1 information
----------------------------------------------------------------
 Admin status         : enable
 Role                 : root
 State                : forwarding
 External path cost   : 100000
 Internal path cost   : 100000
 Priority             : 128
 Designated cost      : 200000
 Designated port      : 128.24
 Designated root      : 32768.0.0000ABCD0000
 Designated bridge    : 32768.0.0030F1552000
 Fast forwarding      : disable
 Forward transitions  : 1
 Admin edge port      : enable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point
 Spanning Tree Status : enable
.
.
.
```

3.3.5 Configuring Interface Settings for MSTP

You can configure the STA interface settings for an MST Instance using the MSTP Port Configuration and MSTP Trunk Configuration pages.

Field Attributes

Read Only Attributes

STA State – Displays current state of this port within the Spanning Tree. (For more information, refer to section **3.1.5 Displaying Interface Settings**.)

- Discarding - Port receives STA configuration messages, but does not forward packets.
- Learning - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
- Forwarding - Port forwards packets, and continues learning addresses.

Trunk – Indicates if a port is a member of a trunk. (STA Port Configuration only)

Configuration Attributes

MST Instance ID – Instance identifier to configure. (Range: 0-4094; Default: 0)

Priority – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (For example, lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

- Default: 128
- Range: 0-240, in steps of 16

MST Path Cost – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (section **9.9.1**), the maximum path cost is 65,535.

Range:

- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

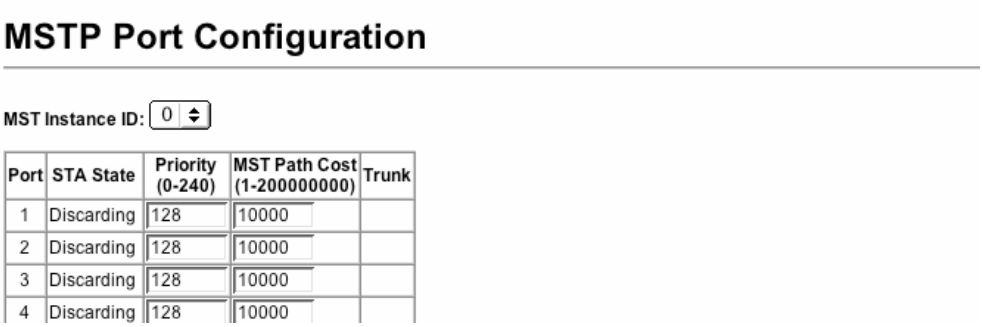
Default:

- Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000

Configuring Switch Using the Web or CLI

Web

Click Spanning Tree – MSTP, Port Configuration or Trunk Configuration. Enter the priority and path cost for an interface, and click Apply.


MSTP Port Configuration
MST Instance ID: 0
Port STA State Priority (0-240) MST Path Cost (1-200000000) Trunk
1 Discarding 128 10000
2 Discarding 128 10000
3 Discarding 128 10000
4 Discarding 128 10000

CLI

This example sets the MSTP attributes for port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#spanning-tree mst port-priority 0
Console(config-if)#spanning-tree mst cost 50
Console(config-if)
```

Chapter 4: Configuring SNTP

You can configure the switch to send time synchronization requests to specific time servers (For example, client mode), update its clock based on broadcasts from time servers, or use both methods. When both methods are enabled, the switch will update its clock using information broadcast from time servers, but will query the specified server(s) if a broadcast is not received within the polling interval.

4.1 SNTP Attributes

SNTP Client – Configures the switch to operate as an SNTP unicast client. This mode requires at least one time server to be specified in the SNTP Server field. (Default: Disabled)

SNTP Broadcast Client – Configures the switch to operate as an SNTP broadcast client. This mode requires no other configuration settings; the switch will obtain time updates from time server broadcasts (using the multicast address 224.0.1.1). (Default: Disabled)

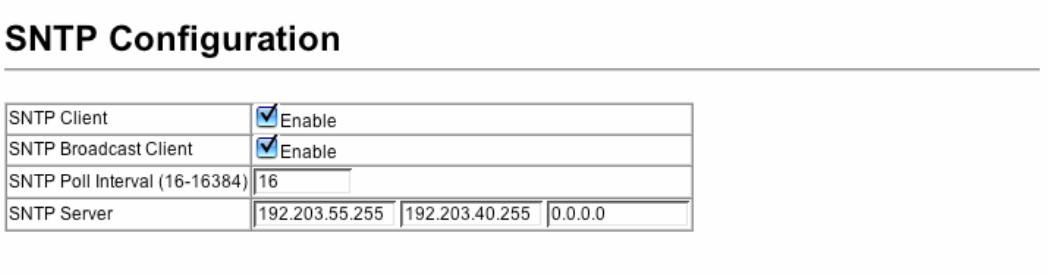
SNTP Poll Interval – Sets the interval between sending requests for a time update from a time server when set to SNTP Client mode. (Range: 16-16284 seconds; Default: 16 seconds)

SNTP Server – In unicast mode, sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

Configuring Switch Using the Web or CLI

Web

Click SNTP – Configuration. Modify any of the required parameters, and click Apply.



CLI

This example configures the switch to operate as an SNTP broadcast client.

```
Console(config)#sntp client
Console(config)#sntp poll 16
Console(config)#sntp server 10.1.0.19 137.82.140.80 128.250.36.2
Console(config)#sntp broadcast client
Console(config)#
```

4.2 Setting the Time Zone

SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

4.2.1 Attributes

Current Time – Displays the current time.

Name – Assigns a name to the time zone.

Hours (0-12) – The number of hour's before/after UTC.

Minutes (0-59) – The number of minute's before/after UTC.

Direction – Configures the time zone to be before (east) or after (west) UTC.

Configuring Switch Using the Web or CLI

Web

Select SNTP – Clock Time Zone. Set the offset for your time zone relative to the UTC, and click Apply.

CLI

This example shows how to set the time zone for the system clock.

```
Console(config)#clock timezone PDT hours 7 minute 0 after-UTC
Console#
```

Chapter 5: Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

The switch includes an onboard SNMP agent that continuously monitors the status of its hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as HP OpenView. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication. The options for configuring community strings, trap functions, and restricting access to clients with specified IP, addresses are described in the following sections.

5.1 Setting Community Access Strings

You may configure up to five community strings authorized for management access. All community strings used for IP Trap Managers should be listed in this table. For security reasons, you should consider removing the default strings.

5.1.2 Attributes

SNMP Community Capability – Indicates that the switch supports up to five community strings.

Community String – A community string that acts like a password and permits access to the SNMP protocol.

Default strings: “public” (read-only access), “private” (read/write access)

Range: 1-32 characters, case sensitive

Access Mode

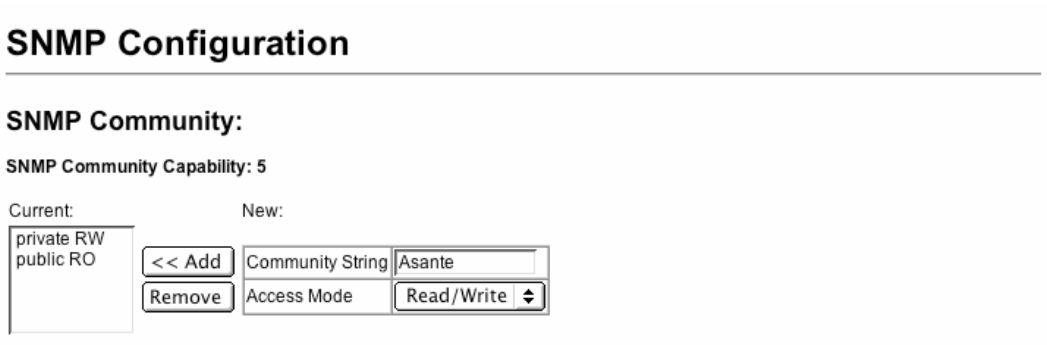
Read-Only – Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

Read/Write – Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Configuring Switch Using the Web or CLI

Web

Click SNMP – Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click Add.



CLI

The following example adds the string “james” with read/write access.

```
Console(config)#snmp-server community james rw
Console(config)#
```

5.2 Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as HP OpenView). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

5.2.1 Attributes

Trap Manager Capability – This switch supports up to five trap managers.

Trap Manager IP Address – Internet address of the host (the targeted recipient).

Trap Manager Community String – Community string sent with the notification operation. (Range: 1-32 characters, case sensitive)

Trap Version – Specifies whether to send notifications as SNMP v1 or v2c traps. (The default is version 1.)

Enable Authentication Traps – Issues a trap message whenever an invalid community string is submitted during the SNMP access authentication process. (The default is enabled.)

Enable Link-up and Link-down Traps – Issues link-up or link-down traps. (The default is enabled.)

Configuring Switch Using the Web or CLI

Web

Click SNMP – Configuration. Fill in the IP address and community string for each trap manager that will receive these messages, specify the SNMP version, mark the trap types required, and then click Add.

CLI

This example adds a trap manager and enables both authentication and link-up, link-down traps.

```
Console(config)#snmp-server host 192.168.1.19 private version 2c
Console(config)#snmp-server enable traps
```

Chapter 6: Configuring Security

You can restrict management access to this switch using the following options:

User Accounts – Manually configure access rights on the switch for specified users.

Authentication Settings – Use remote authentication to configure access rights.

HTTPS Settings – Provide a secure web connection.

SSH Settings – Provide a secure shell (for secure Telnet access).

Port Security – Configure secure addresses for individual ports.

802.1x – Use IEEE 802.1x port authentication to control access to specific ports.

Access Control Lists – provide packet filtering for IP frames.

IP Filter – Filters management access to the web, SNMP or Telnet interface.

6.1 Configuring User Accounts

The guest only has read access for most configuration parameters. The administrator has write access for all parameters governing the onboard agent. You should assign a new administrator password, and store it in a safe place.

The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.”

Configuring Switch Using the CLI

CLI

Assign a user name to access-level 15 (For example, administrator), then specify the password.

```
Console(config)#username james access-level 15
Console(config)#username james password 0 smith
Console(config)#
```

6.2 Configuring Local/Remote Logon Authentication

Use the Authentication Settings menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on RADIUS or TACACS+ protocols.

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

6.2.1 Usage Guidelines

By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via the console port, web browser, or Telnet.

RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.

You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

6.2.2 Command Attributes

Authentication – Select the authentication, or authentication sequence required:

Local – User authentication is performed only locally by the switch.

Radius – User authentication is performed using a RADIUS server only.

TACACS – User authentication is performed using a TACACS+ server only.

[authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.

6.2.3 RADIUS Settings

Server IP Address – Address of authentication server. (Default: 0.0.0.0)

Server Port Number – Network (UDP) port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)

Secret Text String – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Number of Server Transmits – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)

Timeout for a reply – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

6.2.4 TACACS Settings

Server IP Address – Address of the TACACS+ server. (Default: 0.0.0.0)

Server Port Number – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)

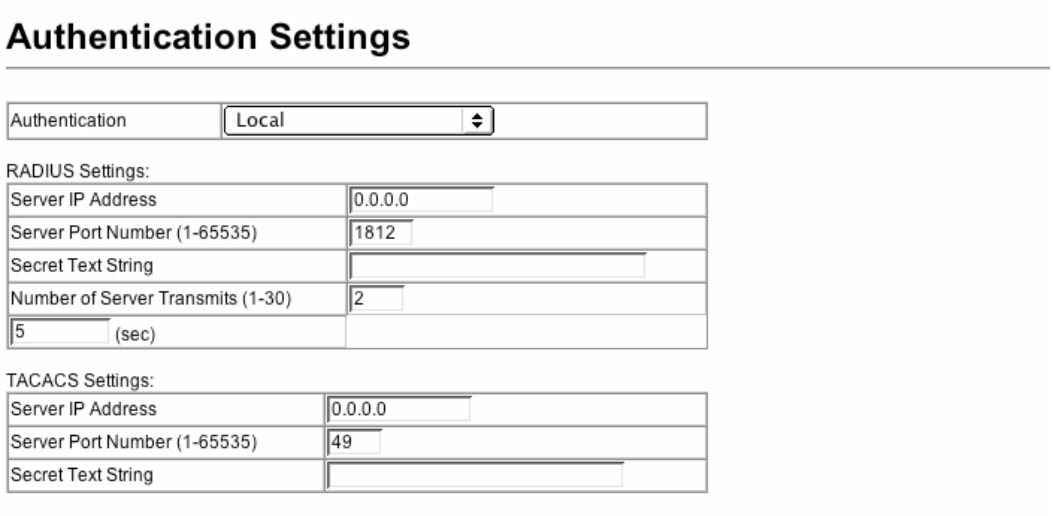
Secret Text String – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI. (See the **username** command in Chapter 16.)

Configuring Switch Using the Web or CLI

Web

Click Security – Authentication Settings. To configure local or remote authentication preferences, specify the authentication sequence (For example, one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click Apply.



CLI

Specify all the required parameters to enable logon authentication.

```
Console#show radius-server
Remote radius server configuration:
 Server IP address: 0.0.0.0
 Communication key with radius server:
 Server port number: 1812
 Retransmit times: 5
 Request timeout: 10
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address: 0.0.0.0
 Communication key with tacacs server: green
 Server port number: 200
Console#
```

6.3 Configuring HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (For example, an encrypted connection) to the switch's web interface.

6.3.1 Usage Guidelines

Both the HTTP and HTTPS service can be enabled independently on the switch. You cannot configure both services to use the same UDP port.

If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://device[:port_number]

- When you start HTTPS, the connection is established in this way:
- The client authenticates the server using the server's digital certificate.
- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.

The client and server establish a secure encrypted connection.

A padlock icon should appear in the status bar for Internet Explorer 5.x or above and Netscape Navigator 4.x or above.

The following web browsers and operating systems currently support HTTPS:

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

To specify a secure-site certificate, see section **6.3.2 Replacing the Default Secure-site Certificate**.

Command Attributes

HTTPS Status – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)

Change HTTPS Port Number – Specifies the UDP port number used for HTTPS/SSL connection to the switch's web interface. (Default: Port 443)

Configuring Switch Using the Web or CLI

Web

Click Security – HTTPS Settings. Enable HTTPS and specify the port number, then click Apply.

CLI

This example enables the HTTP secure server and modifies the port number.

```
Console(config)#ip http secure-server
Console(config)#ip http secure-port 441
Console(config)#
```

6.3.2 Replacing the Default Secure-site Certificate

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

Caution: For maximum security, obtain a unique Secure Sockets Layer certificate at the earliest opportunity. The default certificate for the switch is not unique.

When you have obtained these, place them on your TFTP server, and use the following command at the switch's command-line interface to replace the default (unrecognized) certificate with an authorized one:

```
Console#copy tftp https-certificate
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

Note: The switch must be reset for the new certificate to be activated. To reset the switch, type: Console**#reload**

6.4 Configuring the Secure Shell

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as rlogin (remote login), rsh (remote shell), and rcp (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

Note that you need to install an SSH client on the management station to access the switch for management via the SSH protocol.

Note: The switch supports both SSH Version 1.5 and 2.0.

6.4.1 Usage Guidelines

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified on the Authentication Settings Page (section **6.2 Configuring Local/Remote Logon Authentication**). If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch (SSH Host Key Settings) and enable the SSH server (Authentication Settings).

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – On the SSH Host Key Settings page, create a host public/private key pair.

2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

```
10.1.0.54 1024 35 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167097480477611 7
```

3. Import Client's Public Key to the Switch – Use the copy tftp public-key command (section **15.2.1**) to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch via the User Accounts page as described in section **6.1 Configuring User Accounts**.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA Version 1 key:

```
1024 35 134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19
```

4. Set the Optional Parameters – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. Enable SSH Service – On the SSH Settings page, enable the SSH server on the switch.

6. Challenge-Response Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access. The following exchanges take place during this process:

   - The client sends its public key to the switch.
   - The switch compares the client's public key to those stored in memory.
   - If a match is found, the switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.
   - The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.
   - The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. You do not need to configure the client's keys.

Note: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

6.4.2 Generating the Host Key Pair

A host public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the proceeding section (Usage).

Field Attributes

Public-Key of Host-Key – The public key for the host.

- RSA (Version 1): The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus.
- DSA (Version 2): The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.
- Host-Key Type – The key type used to generate the host key pair (For example, public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both: Default: RSA)

The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

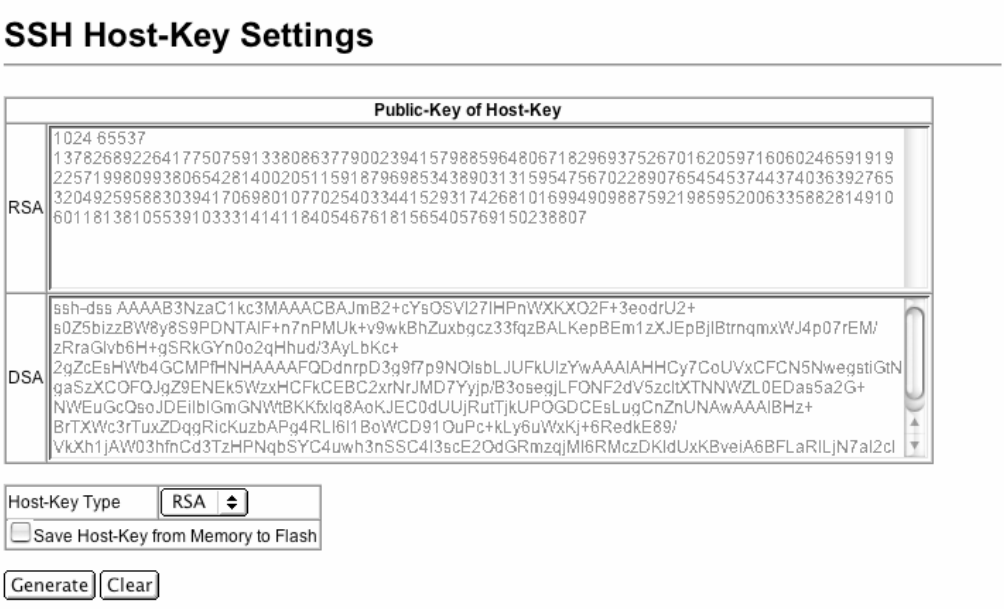
Save Host-Key from Memory to Flash – Saves the host key from RAM (For example, volatile memory to flash memory. Otherwise, the host key pair is stored to RAM by default. Before generating the host-key pair, you must select this item.

Generate – This button is used to generate the host key pair. Note that you must first generate the host key pair before you can enable the SSH server on the SSH Server Settings page.

Configuring Switch Using the Web or CLI

Web

Click Security – SSH Host-Key Settings. Select the host-key type from the drop-down box, select the option to save the host key from memory to flash (if required) before generating the key, and then click Generate.



Host-Key Type: RSA

Save Host-Key from Memory to Flash

Generate Clear

CLI

This example generates a host-key pair using both the RSA and DSA algorithms, stores the keys to flash memory, and then displays the host's public keys.

```
Console#ip ssh crypto host-key generate
Console#ip ssh save host-key
Console#show public-key host
Host:
RSA:
1024 65537 12725092254492640213133651454613118967905519236007602865300676l
82409690947448320102524878965977592168322225584652387791546479807396314033869 25
79310510576521224305280786588548578927260293786608923684142327591212760325919 68
36970534393364384452233351882871738968945117292905108139196420251909321043285 79
045764891
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVXlME1sHL0EcE/Re6hlasfEthIwmj
hLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIICuKg6vjO9XTs7XKc05xfzkBiKviDa
+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6DkZAAAAFQCNZn/x17dwpW8RrV
DQnSWw4Qk+6QAAAIEAptkGeB6B5hwagH4gUOCY6i1TmrmSiJgfwO9OqRPUMbCAkCC+uzxatOo7drnIZ
ypMx+Sx5RUdMGgKS+9ywsa1cWqHeFY5ilc3lDCNBueeLykZzVS+RS+azTKIk/zrJh8GLG
Nq375R55yRxFvmcGIn/Q7IphPqyJ3o9MK8LFDfmJEAAACAL8A6tESiswP2OFqX7VGoEbzVDSOI
RTMFy3iUXtvGyQAOVSy67Mfc3lMtgqPRUOYXDiwIBp5NXgilCg5z7VqbmRm28mWc5a//f8TUAg
PNWKV6W0hqmshQdotVzDR1e+XKNTZj0uTwWfjO5Kytdn4MdoTHgrbl/DMdAfjnte8MZZs=

Console#
```

6.4.3 Configuring the SSH Server

The SSH server includes basic settings for authentication.

Field Attributes

SSH Server Status – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)

Version – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access through SSH either Version 1.5 or 2.0 clients.

SSH Authentication Timeout – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt.

(Range: 1 to 120 seconds; Default: 120 seconds)

SSH Authentication Retries – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)

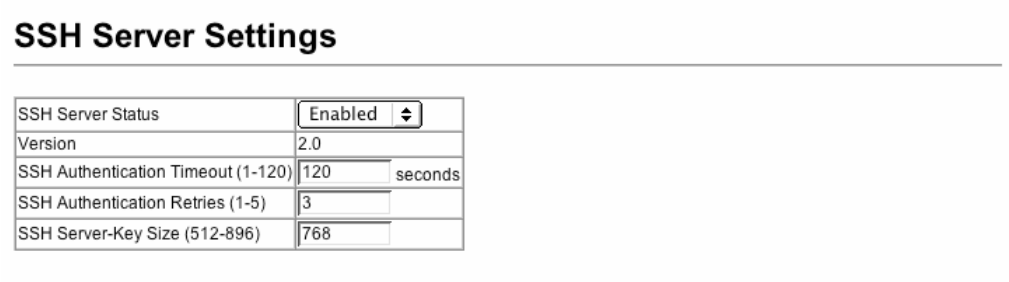
SSH Server-Key Size – Specifies the SSH server key size. (Range: 512-896 bits)

- The server key is a private key that is never shared outside the switch.
- The host key is shared with the SSH client, and is fixed at 1024 bits.

Configuring Switch Using the Web or CLI

Web

Click Security – SSH, Settings. Enable SSH and adjust the authentication parameters as required, then click Apply. Note that you must first generate the host key pair on the SSH Host-Key Settings page before you can enable the SSH server.



CLI

This example enables SSH, sets the authentication parameters, and displays the current configuration. It shows that the administrator has made a connection through SHH, and then disables this connection.

```
Console(config)#ip ssh server
Console(config)#ip ssh timeout 100
Console(config)#ip ssh authentication-retries 5
Console(config)#ip ssh server-key size 512
Console(config)#end
Console#show ip ssh
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#show ssh
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin   2.0      cipher-3des   session-started
Console#disconnect 0
Console#
```

6. 5 Configuring Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port. Note that you can also restrict the maximum number of addresses that can be learned by a port.

To add new VLAN members later, you can manually add secure addresses with the Static Address Table (section **8.1 Setting Static Addresses**), or turn off port security to reenable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.

6.5.1 Guidelines

A secure port has the following restrictions:

- Cannot use port monitoring.
- Cannot be a multi-VLAN port.
- Cannot be used as a member of a static or dynamic trunk.
- Should not be connected to a network interconnection device.

If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Port/Port Configuration page (see section **7.2 Configuring Interface Connections**).

Command Attributes

Port – Port number.

Name – Descriptive text.

Action – Indicates the action to be taken when a port security violation is detected:

- None: No action should be taken. (This is the default.)
- Trap: Send an SNMP trap message.
- Shutdown: Disable the port.
- Trap and Shutdown: Send an SNMP trap message and disable the port.

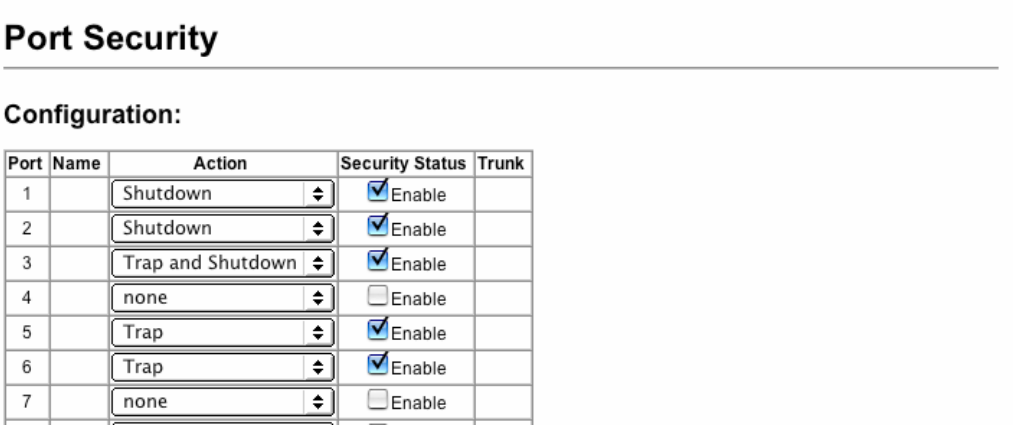
Security Status – Enables or disables port security on the port. (Default: Disabled)

Trunk – Trunk number if port is a member (section **9.9.1**).

Configuring Switch Using the Web or CLI

Web

Click Security – Port Security. Set the action to take when an invalid address is detected on a port, mark the checkbox in the Status column to enable security for a port and click Apply.



CLI

This example sets the command mode to Port 5, sets the port security action to send a trap and disable the port, and then enables port security for the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown
Console(config-if)#port security
Console(config-if)#
```

6.6 Configuring 802.1x Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1x (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (For example, Supplicant) connects to a switch port, the switch (For example, Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but also the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The authentication method currently supported is MD5 only. The client responds to the appropriate method with its password. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

The operation of 802.1x on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- Each switch port that will be used must be set to dot1x “Auto” mode.

- Each client that needs to be authenticated must have dot1x client software installed and properly configured.

- The RADIUS server and 802.1x client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)

- The RADIUS server and client also have to support the same EAP authentication type – MD5, (Some clients have native support in Windows, otherwise the dot1x client must support it.)

6.6.1: Displaying 802.1x Global Settings

The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (For example, authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

Command Attributes

802.1X Re-authentication – Indicates if switch port requires a client to be re-authenticated after a certain period.

802.1X Max Request Count – The maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session.

Timeout For Quiet Period – Indicates the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client.

Timeout For Re-authentication Period – Indicates the time after which a connected client must be re-authenticated.

Timeout For Tx Period – The period during an authentication session that the switch waits before re-transmitting an EAP packet.

Supplicant Timeout – The time the switch waits for a client response to an EAP request.

Server Timeout – The time the switch waits for a response from the authentication server (RADIUS) to an authentication request.

Re-authentication Max Count – The number of times the switch will attempt to re-authenticate a connected client before the port becomes unauthorized.

Configuring Switch Using the Web or CLI

Web

Click Security – 802.1x, Information.

802.1x Information

802.1x Re-authentication	Enable
Disabled	
802.1x Max Request Count	2
2	
Timeout for Quiet Period	60 seconds
60 seconds	
Timeout for Re-authentication Period	3600 seconds
3600 seconds	
Timeout for Tx Period	30 seconds
30 seconds	
Supplicant Timeout	30 seconds
Server Timeout	10 seconds
Re-authentication Max Count	2

CLI

This example shows the default protocol settings for 802.1x. For a description of the additional entries displayed in the CLI, See the **show dot1x** command.

```
Console#show dot1x
Global 802.1X Parameters
 reauth-enabled: yes
 reauth-period:  3600
 quiet-period:   60
 tx-period:      30
 supp-timeout:   30
 server-timeout: 30
 reauth-max:     2
 max-req:        2

802.1X Port Summary
 Port Name     Status     Operation Mode                Mode     Authorized
       1/1   disabled        Single-Host      ForceAuthorized            n/a
       1/2   disabled        Single-Host      ForceAuthorized            n/a
.
.
.
      1/47   disabled        Single-Host      ForceAuthorized            n/a
      1/48   enabled         Single-Host                 Auto             yes

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is disabled on port 1/2
.
.
.
.

802.1X is disabled on port  1/47

802.1X is enabled on port  1/48
Status              Authorized
Operation mode      Single-Host
Max count           5
```

```
Port-control        Auto
Supplicant          00-00-e8-49-5e-dc
Current Identifier  3

Authenticator State Machine
State               Authenticated
Reauth Count        0

Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  2

Reauthentication State Machine
State               Initialize
Console#
```

6.6.2 Configuring 802.1x Global Settings

The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (For example, authenticator), as well as the client identity lookup process that runs between the switch and authentication server. The configuration options for parameters are described in this section.

Command Attributes

802.1X Re-authentication – Sets the client to be re-authenticated after the interval specified by the Timeout for Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)

802.1X Max Request Count – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)

Timeout For Quiet Period – Sets the time that a switch port waits after the dot1X Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)

Timeout For Re-authentication Period – Sets the time after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)

Timeout For Tx Period – Sets the time during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)

authentication dot1x default (CLI only) – Sets the default authentication server type. Note that the specified authentication server type must be enabled and properly configured for dot1x to function properly. (Options: radius).

Configuring Switch Using the Web or CLI

Web

Select Security – 802.1x, Configuration. Enable dot1x globally for the switch, modify any of the parameters required, and then click Apply.

CLI

This enables re-authentication and sets all of the global parameters for 802.1x.

```
Console(config)#dot1x re-authentication
Console(config)#dot1x max-req 5
Console(config)#dot1x timeout quiet-period 40
Console(config)#dot1x timeout re-authperiod 5
Console(config)#dot1x timeout tx-period 40
Console(config)#authentication dot1x default radius
Console(config)#
```

6.6.3 Configuring Port Authorization Mode

When dot1x is enabled, you need to specify the dot1x authentication mode configured for each port.

Command Attributes

Status – Indicates if authentication is enabled or disabled on the port.

Operation Mode – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Range: Single-Host, Multi-Host; Default: Single-Host)

Max Count – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-20; Default: 5)

Mode – Sets the authentication mode to one of the following options:

- Auto – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
- Force-Authorized – Forces the port to grant access to all clients, either dot1x-aware or otherwise.
- Force-Unauthorized – Forces the port to deny access to all clients, either dot1x-aware or otherwise.

Authorized – Sets the authorization:

- Yes – Connected client is authorized.
- No – Connected client is not authorized.
- Blank – Displays nothing when dot1x is disabled on a port.

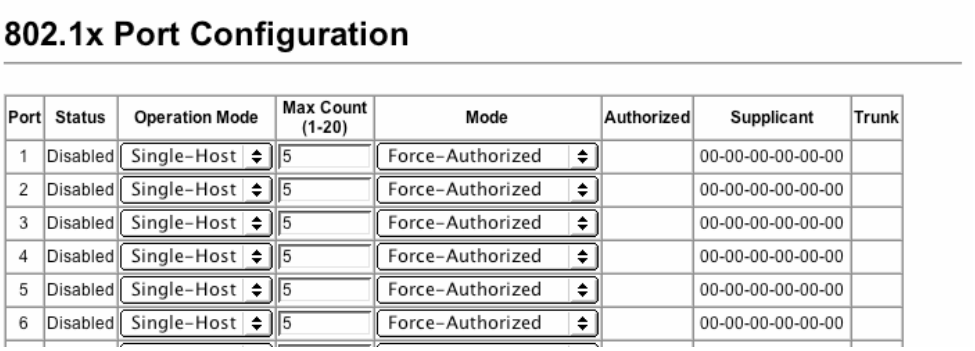
Supplicant – Indicates the MAC address of a connected client.

Trunk – Indicates if the port is configured as a trunk port.

Configuring Switch Using the Web or CLI

Web

Click Security – 802.1x, Port Configuration. Select the authentication mode from the drop-down box and click Apply.



CLI

This example sets the authentication mode to enable 802.1x on port 2, and allows up to ten clients to connect to this port.

```
Console(config)#interface ethernet 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

6.6.4 Displaying 802.1x Statistics

This switch can display statistics for dot1x protocol exchanges for any port.

The following table lists the parameters and descriptions for the 802.1x statistical values

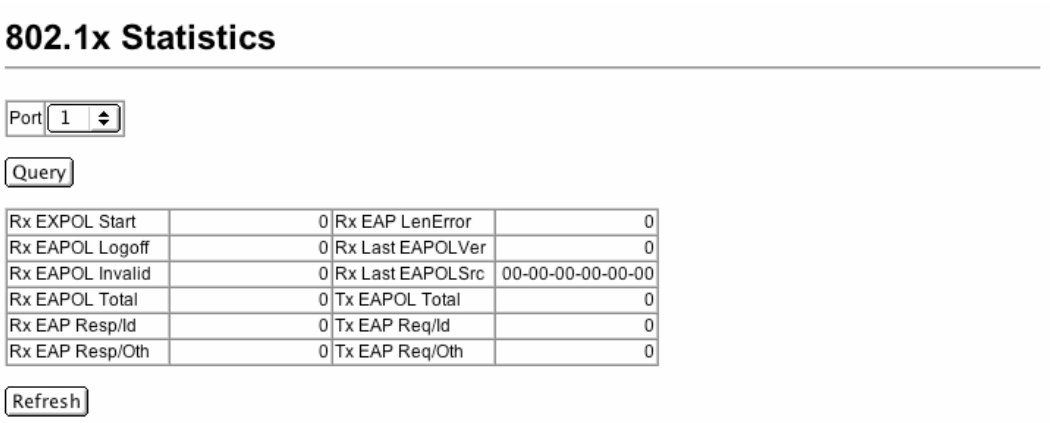
Parameter	Description
Rx EXPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in

	which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Configuring Switch Using the Web or CLI

Web

Select Security – 802.1x, Statistics. Select the required port and then click Query. Click Refresh to update the statistics.



CLI

This example displays the 802.1x statistics for port 4.

```
Console#show dot1x statistics interface ethernet 1/4

Eth 1/4
Rx: EAPOL      EAPOL      EAPOL      EAPOL      EAP      EAP      EAP
    Start      Logoff     Invalid    Total      Resp/Id  Resp/Oth LenError
        2          0          0       1007       672        0        0

    Last       Last
EAPOLVer     EAPOLSrc
       1     00-00-E8-98-73-21

Tx: EAPOL      EAP      EAP
    Total      Req/Id   Req/Oth
     2017      1005        0
```

```
Console#
```

6.7 Configuring Access Control Lists

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

6.7.1 Guidelines

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

The following restrictions apply to ACLs:

Each ACL can have up to 32 rules.

The maximum number of ACLs is also 32.

The average number of rules bound to the ports should not exceed 20.

You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.

The switch does not support the explicit “deny any any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Egress MAC ACL for egress ports.
2. User-defined rules in the Egress IP ACL for egress ports.
3. User-defined rules in the Ingress MAC ACL for ingress ports.
4. User-defined rules in the Ingress IP ACL for ingress ports.
5. Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
6. Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.
7. If no explicit rule is matched, the implicit default is permit all.

6.7.2 Setting the ACL Name and Type

Use the ACL Configuration page to designate the name and type of an ACL.

Command Attributes

Name – Name of the ACL. (Maximum length: 16 characters)

Type – There are three filtering modes:

- Standard: IP ACL mode that filters packets based on the source IP address.
- Extended: IP ACL mode that filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the “TCP” protocol is specified, then you can also filter packets based on the TCP control code.
- MAC: MAC ACL mode that filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Configuring Switch Using the Web or CLI

Web

Click Security – ACL, Configuration. Enter an ACL name in the Name field, select the list type (IP Standard, IP Extended, or MAC), and click Add to open the configuration page for the new list.

CLI

This example creates a standard IP ACL named asante.

```
Console(config)#access-list ip standard asante
Console(config-std-acl)#
```

6.7.3 Configuring a Standard IP ACL

Command Attributes

Action – An ACL can contain all permit rules or all deny rules. (Default: Permit rules)

IP – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)

Address – Source IP address.

SubMask – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The mask is bitwise appended with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Configuring Switch Using the Web or CLI

Web

Specify the action (For example, Permit or Deny). Select the address type (Any, Host, or IP). If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range. Then click Add.

Jaci need picture here Need Breen to help with illo

CLI

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

6.7.4 Configuring an Extended IP ACL

Command Attributes

Action – An ACL contains either all permit rules or all deny rules. (Default: Permit rules)

Src/Dst IP – Specifies the source or destination IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)

Src/Dst Address – Source or destination IP address.

Src/Dst SubMask – Subnet mask for source or destination address. (See the description for SubMask in section **6.7.3 Configuring a Standard IP ACL**.)

Service Type – Packet priority settings based on the following criteria:

- Precedence – IP precedence level. (Range: 0-7)
- TOS – Type of Service level. (Range: 0-15)
- DSCP – DSCP priority level. (Range: 0-64)

Protocol – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)

Src/Dst Port – Source/destination port number for the specified protocol type. (Range: 0-65535)

Src/Dst Port Bitmask – Decimal number representing the port bits to match. (Range: 0-65535)

Control Code – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

Control Bitmask – Decimal number representing the code bits to match.

The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

- 1 (fin) – Finish
- 2 (syn) – Synchronize
- 4 (rst) – Reset
- 8 (psh) – Push
- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

SYN flag valid, use control-code 2, control bitmask 2

Both SYN and ACK valid, use control-code 18, control bitmask 18

SYN valid and ACK invalid, use control-code 2, control bitmask 18

Configuring Switch Using the Web or CLI

Web

Specify the action (For example, Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or IP). If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range. Set any other required criteria, such as service type, protocol type, or TCP control code. Then click Add.

Jaci need pic here 3-29 Need Breen to help

CLI

This example adds three rules:

- Accept any incoming packets if the source address is in subnet 10.7.1.x. For example, if the rule is matched; For example, the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.
- Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (For example, HTTP).
- Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN”.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port
80
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  control-flag 2 2
Console(config-ext-acl)#
```

6.7.5 Configuring a MAC ACL

Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

Command Attributes

Action – An ACL can contain all permit rules or all deny rules. (Default: Permit rules)

Source/Destination MAC – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Bitmask fields. (Options: Any, Host, MAC; Default: Any)

Source/Destination MAC Address – Source or destination MAC address.

Source/Destination MAC Bitmask – Hexadecimal mask for source or destination MAC address.

VID – VLAN ID. (Range: 1-4094)

VID Mask – VLAN bitmask. (Range: 1-4094)

Ethernet Type – This option can only be used to filter Ethernet II formatted packets. (Range: 600-fff hex.)

A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the common types include 0800 (IP), 0806 (ARP) and 8137 (IPX).

Ethernet Type Mask – Protocol bitmask. (Range: 600-fff hex.)

Packet Format – This attribute includes the following packet types:

- Any – Any Ethernet packet type.
- Untagged-eth2 – Untagged Ethernet II packets.
- Untagged-802.3 – Untagged Ethernet 802.3 packets.
- Tagged-eth2 – Tagged Ethernet II packets.
- Tagged-802.3 – Tagged Ethernet 802.3 packets.

Configuring Switch Using the Web or CLI

Web

Specify the action (For example, Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or MAC). If you select “Host,” enter a specific address (e.g., 11-22-33-44-55-66). If you select “MAC,” enter a base address and a hexadecimal bitmask for an address range. Set any other required criteria, such as VID, Ethernet type, or packet format. Then click Add.

Jaci need pic here 3-30 Need breen to help

CLI

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

6.7.6 Configuring ACL Masks

You can specify optional masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ingress or egress ACL. A mask must be bound exclusively to one of the basic ACL types (For example, Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Follow these guidelines:

Up to seven entries can be assigned to an ACL mask.

Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules are entered.

Create the required ACLs and the ingress or egress masks before mapping an ACL to an interface.

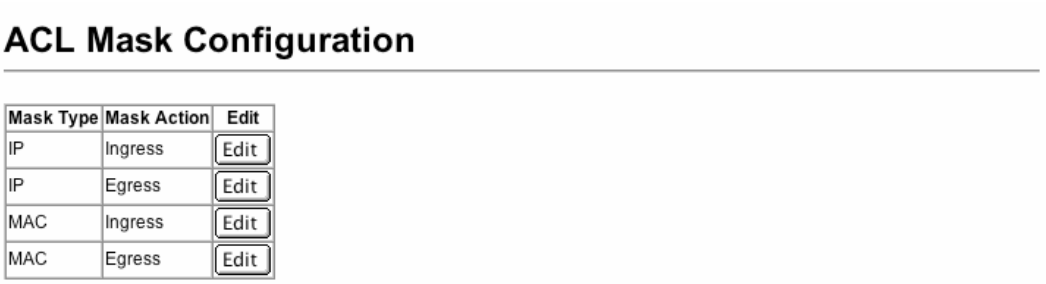
You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

Use the ACL Mask Configuration page to edit the mask for the Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL.

Configuring Switch Using the Web or CLI

Web

Click Security – ACL, Mask Configuration. Click Edit for one of the basic mask types to open the configuration page.



CLI

This example creates an IP ingress mask, and then adds two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

6.7.7 Configuring an IP ACL Mask

This mask defines the fields to check in the IP header.

Follow these guidelines.

Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Command Attributes

Src/Dst IP – Specifies the source or destination IP address. Use “Any” to match any address, “Host” to specify a host address (not a subnet), or “IP” to specify a range of addresses. (Options: Any, Host, IP; Default: Any)

Src/Dst IP Bitmask – Source or destination address of rule must match this bitmask. (See the description for SubMask in section **6.7.3 Configuring a Standard IP ACL.**)

Protocol Bitmask – Check the protocol field.

Service Type – Check the rule for the specified priority type. (Options: Precedence, TOS, DSCP; Default: TOS)

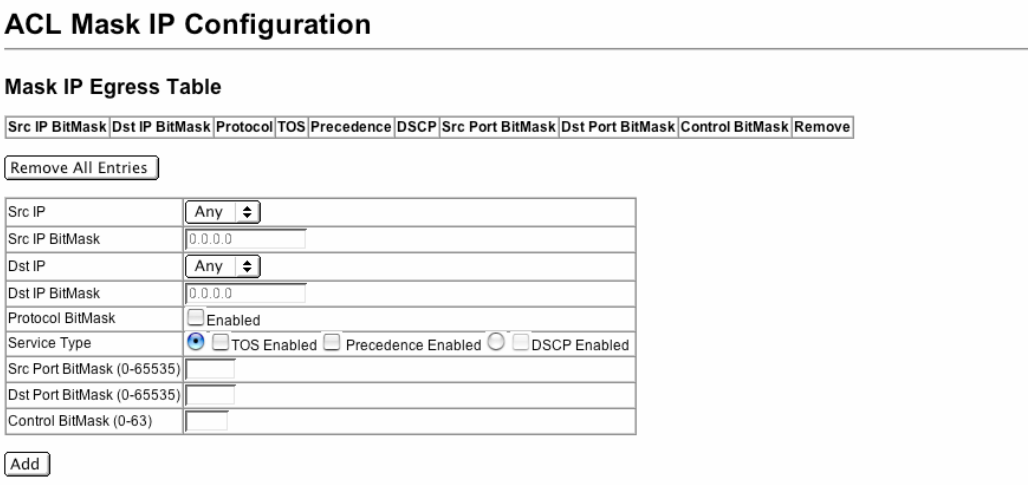
Src/Dst Port Bitmask – Protocol port of rule must match this bitmask. (Range: 0-65535)

Control Bitmask – Control flags of rule must match this bitmask. (Range: 0-63)

Configuring Switch Using the Web or CLI

Web

Configure the mask to match the required rules in the IP ingress or egress ACLs. Set the mask to check for any source or destination address, a specific host address, or an address range. Include other criteria to search for in the rules, such as a protocol type or one of the service types. Alternatively, use a bitmask to search for specific protocol port(s) or TCP control code(s). Then click Add.



CLI

This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the “deny 10.1.1.1 255.255.255.255” rule has the higher precedence according the “mask host any” entry.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0
```

```
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

6.7.8 Configuring a MAC ACL Mask

This mask defines the fields to check in the packet header.

Follow these guidelines.

You must configure a mask for an ACL rule before you can bind it to a port.

Command Attributes

Source/Destination MAC – Use “Any” to match any address, “Host” to specify the host address for a single node, or “MAC” to specify a range of addresses. (Options: Any, Host, MAC; Default: Any)

Source/Destination MAC Bitmask – Address of rule must match this bitmask.

VID Bitmask – VLAN ID of rule must match this bitmask.

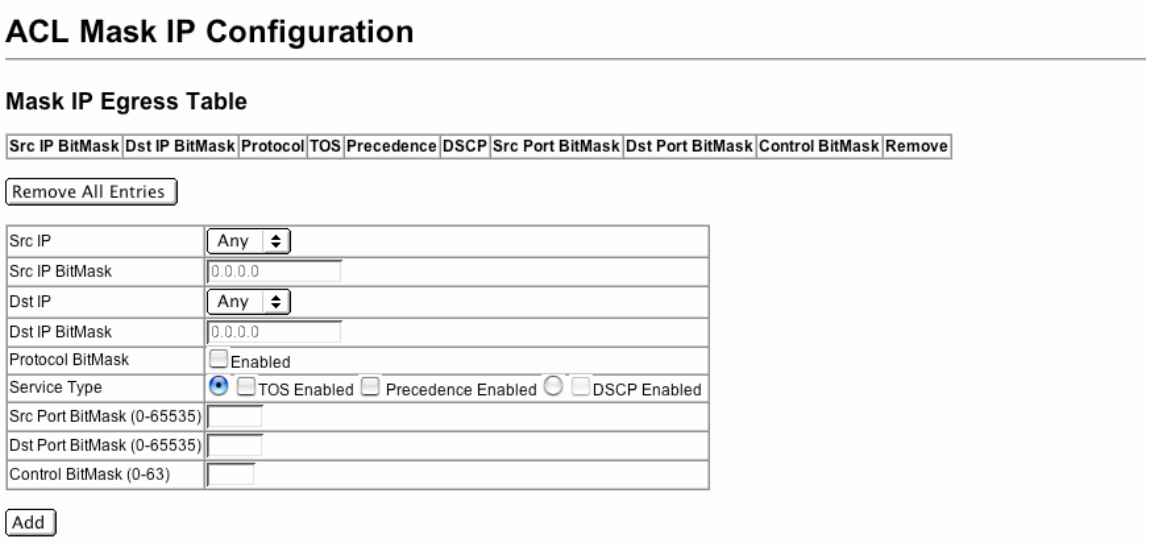
Ethernet Type Bitmask – Ethernet type of rule must match this bitmask.

Packet Format Bitmask – A packet format must be specified in the rule.

Configuring Switch Using the Web or CLI

Web

Configure the mask to match the required rules in the MAC ingress or egress ACLs. Set the mask to check for any source or destination address, a host address, or an address range. Use a bitmask to search for specific VLAN ID(s) or Ethernet type(s). Alternatively, check for rules where a packet format was specified. Then click Add.



CLI

This example shows how to create an Ingress MAC ACL and bind it to a port. You can see the mask has changed the order of the rules.

```
Console(config)#access-list mac M4
Console(config-mac-acl)#permit any any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11 ff-ff-ff-ff-ff-ff
any vid 3
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M4:
  permit any any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#mac access-group M4 in
Console(config-if)#end
Console#show access-list
MAC access-list M4:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
  permit any any
MAC ingress mask ACL:
  mask pktformat host any vid
Console#
```

6.7.9 Binding a Port to an Access Control List

After configuring the Access Control Lists (ACL), you can bind the ports that need to filter traffic to the appropriate ACLs. You can only bind a port to one ACL for each basic type – IP ingress, IP egress, MAC ingress and MAC egress.

Follow these guidelines.

You must configure a mask for an ACL rule before you can bind it to a port.

This switch supports ACLs for both ingress and egress filtering. You can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.

When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.

The switch does not support the explicit “deny any any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

Command Attributes

Port – Fixed port or SFP module. (Range: 1-24, 1-48)

IP – Specifies the IP ACL to bind to a port.

MAC – Specifies the MAC ACL to bind to a port.

IN – ACL for ingress packets.

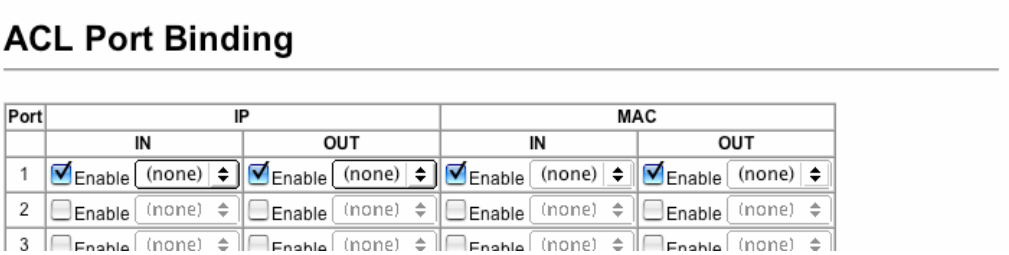
OUT – ACL for egress packets.

ACL Name – Name of the ACL.

Configuring Switch Using the Web or CLI

Web

Click Security – ACL, Port Binding. Mark the Enable field for the port you want to bind to an ACL for ingress or egress traffic, select the required ACL from the drop-down list, then click Apply.



CLI

This examples assigns an IP and MAC ingress ACL to port 1, and an IP ingress ACL to port 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group david in
Console(config-if)#mac access-group jerry in
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

6.8 Configuring IP Filters

The switch allows you to create a web browser list of up to 16 IP addresses or IP address groups that are allowed access to the switch via web browser, SNMP, or Telnet.

6.8.1 Guidelines

To specify the clients allowed management access, enter an IP address to identify a specific host or a range of valid addresses. For example:

- IP address 192.168.1.1 – Specifies a valid IP address of 192.168.1.1 for a single client.

The default setting is null, which allows all IP groups management access to the switch. If one or more IP addresses are configured, IP filtering is enabled and only addresses listed in this table will have management access.

Note: Subnet masks may only be specified at the command line.

Command Attributes

Web IP Filter List – Configures IP address(es) for the web group.

SNMP IP Filter List – Configures IP address(es) for the SNMP group.

Telnet IP Filter List – Configures IP address(es) for the Telnet group.

IP Filter List – IP addresses which are allowed management access to this interface.

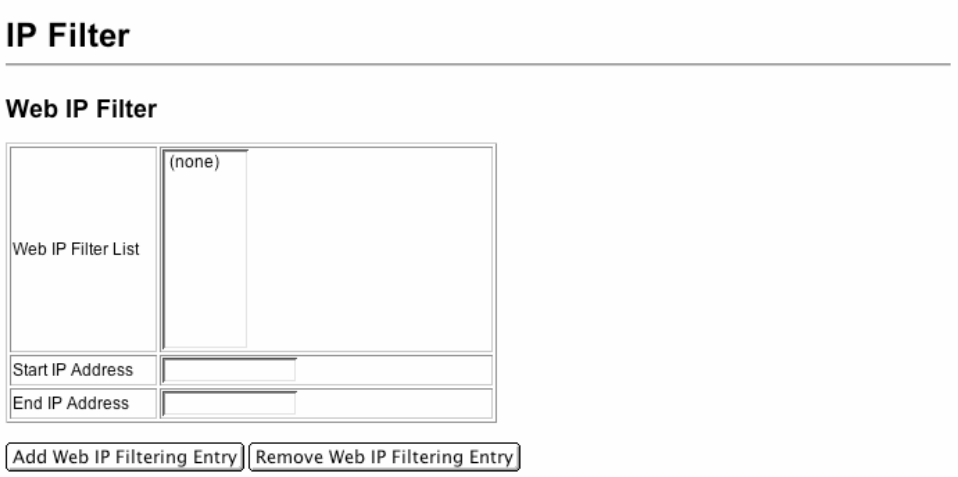
Start IP Address – A single IP address, or the starting address of a range.

End IP Address – The end address of a range.

Configuring Switch Using the Web or CLI

Web

Click Security – IP Filter. Enter the addresses that are allowed management access to an interface, and click Add IP Filtering Entry.



CLI

This example allows SNMP access for a specific client.

```
Console(config)#management snmp-client 10.1.2.3
Console(config)#end
Console#show management all-client
Management Ip Filter
Http-Client:
Start ip address End ip address
-----------------------------------------------

Snmp-Client:
Start ip address End ip address
-----------------------------------------------
1. 10.1.2.3      10.1.2.3
Telnet-Client:
Start ip address End ip address
-----------------------------------------------

Console#
```

Chapter 7: Configuring Ports

7.1 Displaying Connection Status

You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Field Attributes (Web)

Name – Interface label.

Type – Indicates the port type.

(1000BASE-T, 1000BASE-SX, 1000BASE-LX or 100BASE-LH)

Admin Status – Shows if the interface is enabled or disabled.

Oper Status – Indicates if the link is Up or Down.

Speed Duplex Status – Shows the current speed and duplex mode. (Auto, or fixed choice)

Flow Control Status – Indicates the type of flow control currently in use.

(IEEE 802.3x, Back-Pressure or None)

Autonegotiation – Shows if auto-negotiation is enabled or disabled.

Forced Mode1 – Shows the forced/preferred port type to use for combination ports 21-24 or 45-48. (Copper-Forced, Copper-Preferred-Auto, SFP-Forced, SFP-Preferred-Auto)

Trunk Member1 – Shows if port is a trunk member.

Creation2 – Shows if a trunk is manually configured or dynamically set via LACP.

1: Port Information only.

2: Trunk Information only

Configuring Switch Using the Web or CLI

Web

Click Port – Port Information or Trunk Information.

Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Forced Mode	Trunk Member
1		1000Base-T	Enabled	Down	1000full	None	Enabled	None	
2		1000Base-T	Enabled	Down	1000full	None	Enabled	None	
3		1000Base-T	Enabled	Down	1000full	None	Enabled	None	

Field Attributes (CLI)

Basic information

Port type – Indicates the port type. (1000BASE-T, 1000BASE-SX, 1000BASE-LX or 1000BASE-LH)

MAC address – The physical layer address for this port. (To access this item on the web, see section **2.4 Setting an IP Address**.)

Configuration

Name – Interface label.

Port admin – Shows if the interface is enabled or disabled (For example, up or down).

Speed-duplex – Shows the current speed and duplex mode. (Auto, or fixed choice)

Capabilities – Specifies the capabilities to be advertised for a port during auto-negotiation. (To access this item on the web, see section **7.2 Configuring Interface Connections**.) The following capabilities are supported.

- 10half - Supports 10 Mbps half-duplex operation
- 10full - Supports 10 Mbps full-duplex operation
- 100half - Supports 100 Mbps half-duplex operation
- 100full - Supports 100 Mbps full-duplex operation
- 1000full - Supports 1000 Mbps full-duplex operation
- Sym - Transmits and receives pause frames for flow control
- FC - Supports flow control

Broadcast storm – Shows if broadcast storm control is enabled or disabled.

Broadcast storm limit – Shows the broadcast storm threshold. (500 - 262143 packets per second)

Flow control – Shows if flow control is enabled or disabled.

LACP – Shows if LACP is enabled or disabled.

Port Security – Shows if port security is enabled or disabled.

Max MAC count – Shows the maximum number of MAC address that can be learned by a port. (0 - 20 addresses)

Port security action – Shows the response to take when a security violation is detected. (shutdown, trap, trap-and-shutdown)

Combo forced mode – Shows the forced/preferred port type to use for combination ports 21-24 or 45-48. (copper forced, copper preferred auto, SFP forced, SFP preferred auto)

Current status

Link Status – Indicates if the link is up or down.

Operation speed-duplex – Shows the current speed and duplex mode.

Flow control type – Indicates the type of flow control currently in use.

(IEEE 802.3x, Back-Pressure or none)

CLI

This example shows the connection status for Port 5.

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/13
 Basic information:
  Port type: 1000T
  Mac address: 00-30-f1-47-58-46
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
 Current status:
  Link status: Down
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```

7.2 Configuring Interface Connections

You can use the Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

Command Attributes

Name – Allows you to label an interface. (Range: 1-64 characters)

Admin – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.

Speed/Duplex – Allows you to manually set the port speed and duplex mode.

Flow Control – Allows automatic or manual selection of flow control.

Autonegotiation (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control. The following capabilities are supported.

- 10half - Supports 10 Mbps half-duplex operation

- 10full - Supports 10 Mbps full-duplex operation
- 100half - Supports 100 Mbps half-duplex operation
- 100full - Supports 100 Mbps full-duplex operation
- 1000full - Supports 1000 Mbps full-duplex operation
- Sym (Gigabit only) - Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames. (The current switch chip only supports symmetric pause frames.)
- FC - Supports flow control. Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)

  (Default: Autonegotiation enabled; Advertised capabilities for 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; 1000BASE-SX/LX/LH – 1000full)

Forced Mode – Shows the forced/preferred port type to use for the combination ports 21-24 or 45-48.

- Copper-Forced - Always uses the built-in RJ-45 port.
- Copper-Preferred-Auto - Uses the built-in RJ-45 port if both combination types are functioning and the RJ-45 port has a valid link.
- SFP-Forced - Always uses the SFP port (even if module is not installed).
- SFP-Preferred-Auto - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

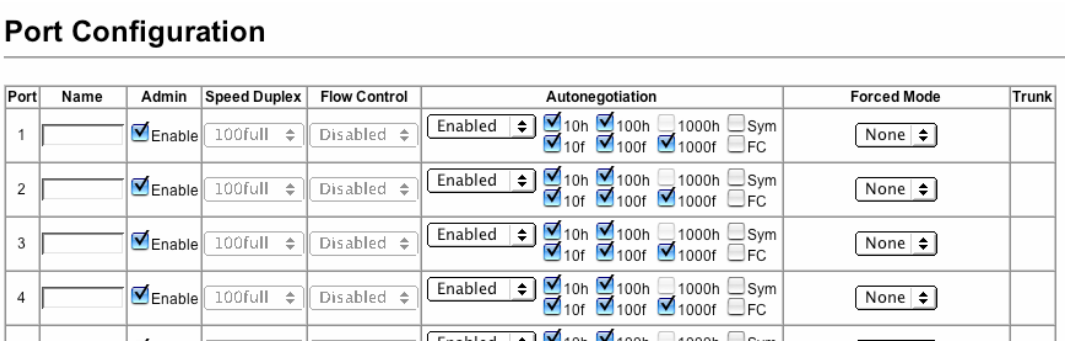
Trunk – Indicates if a port is a member of a trunk. To create trunks and select port members, see section **7.3 Configuring Trunk Groups**.

Note: Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Configuring Switch Using the Web or CLI

Web

Click Port – Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.



CLI

Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13
Console(config-if)#description RD SW#13
Console(config-if)#shutdown
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation
Console(config-if)#speed-duplex 100half
Console(config-if)#flowcontrol
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#exit
Console(config)#interface ethernet 1/21
Console(config-if)#combo-forced-mode copper-forced
Console(config-if)#
```

7.3 Configuring Trunk Groups

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to six trunks at a time.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than four ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Usage Guidelines

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. Before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to six trunks on the switch, with up to eight ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (For example, speed, duplex mode and flow control), VLAN assignments, and CoS settings.

- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.

- STP, VLAN, and IGMP settings can only be made for the entire trunk.

7.3.1 Creating a Static Trunk

When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. The static trunks on this switch are Cisco EtherChannel compatible.

To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and disconnect the ports before removing a static trunk via the configuration interface.

Configuring Switch Using the Web or CLI

Web

Click Port – Trunk Membership. Enter a trunk ID of 1-6 in the Trunk field, select any of the switch ports from the scroll-down port list, and click Add. After you have completed adding ports to the member list, click Apply.

CLI

This example creates trunk 2 with ports 1 and 2. Just connect these ports to two static trunk ports on another switch to form a trunk.

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#channel-group 1
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-AA-AA-01
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control: Disabled
```

```
  Port security: Disabled
  Max MAC count: 0
 Current status:
  Created by: User
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/1, Eth1/2,
Console#
```

7.4 Enabling LACP on Selected Ports

To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.

If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.

A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.

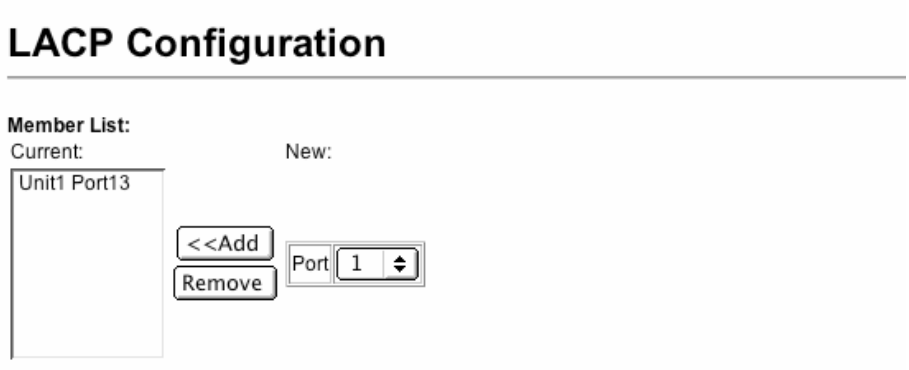
If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

All ports on both ends of an LACP trunk must be configured for full duplex, by forced either mode or auto-negotiation.

Configuring Switch Using the Web or CLI

Web

Click Port – LACP, Configuration. Select any of the switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click Apply.



CLI

The following example enables LACP for ports 1 to 6. Just connect these ports to LACP-enabled trunk ports on another switch to form a trunk.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lacp
Console(config-if)#exit
.
.
.
```

```
Console(config)#interface ethernet 1/6
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 1000T
  Mac address: 22-22-22-22-22-2d
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
 Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6,
Console#
```

7.4.1 Configuring LACP Parameters

Dynamically Creating a Port Channel

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP System Priority.
- Ports must have the same LACP port Admin Key.
- If the “port channel” Admin Key is set (**lacp admin-key** command), then the port Admin Key must be set to the same value for a port to be allowed to join a channel group.

  Note: If the port channel admin key (**lacp admin-key** command) is not set (through the CLI) when a channel group is formed (it has a null value of 0), this key is set to the same value as the port admin key used by the interfaces that joined the group (**lacp admin-key** command as described in Chapter 16).

Command Attributes

Set Port Actor – This menu sets the local side of an aggregate link; For example, the ports on this switch.

Port – Port number. (Range:1-24, 1-48)

System Priority – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)

- Ports must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch’s MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.

Admin Key – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: 0)

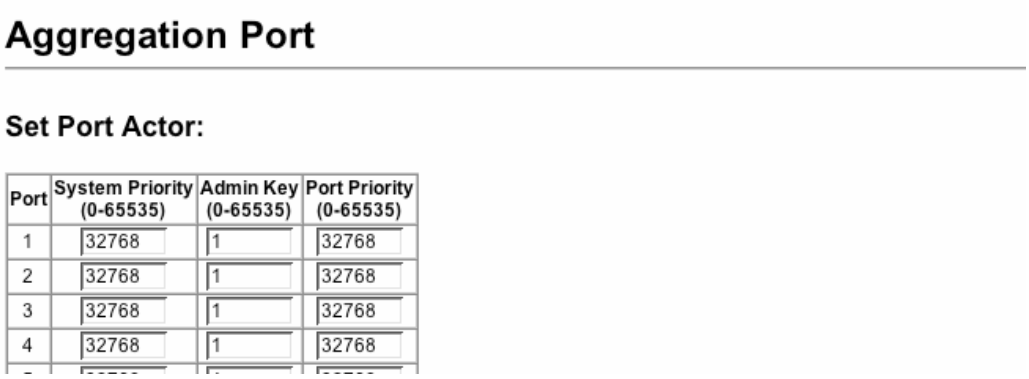
Port Priority – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

Set Port Partner – This menu sets the remote side of an aggregate link; For example, the ports on the attached device. The command attributes have the same meaning as those used for the port actor. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Configuring Switch Using the Web or CLI

Web

Click Port – LACP, Aggregation Port. Set the System Priority, Admin Key, and Port Priority for the Port Actor. You can optionally configure these settings for the Port Partner. (Be aware that these settings only affect the administrative state of the partner, and will not take effect until the next time an aggregate link is formed with this device.) After you have completed setting the port LACP parameters, click Apply.



CLI

The following example configures LACP parameters for ports 1-6. Ports 1-4 are used as active members of the LAG; ports 5 and 6 are set to backup mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 128
Console(config-if)#exit
.
.
.
Console(config)#interface ethernet 1/6
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 512
Console(config-if)#end
Console#show lacp sysid
Channel Group    System Priority    System MAC Address
-------------------------------------------------------------------------
            1              32768     00-00-E9-31-31-31
            2              32768     00-00-E9-31-31-31
            3              32768     00-00-E9-31-31-31
```

```
            4               32768      00-00-E9-31-31-31
            5               32768      00-00-E9-31-31-31
            6               32768      00-00-E9-31-31-31
Console#show lacp 1 internal
Channel group : 1
------------------------------------------------------------------------
Oper Key : 120
Admin Key : 120
Console#
```

7.4.2 Displaying LACP Port Counters

You can display statistics for LACP protocol messages.

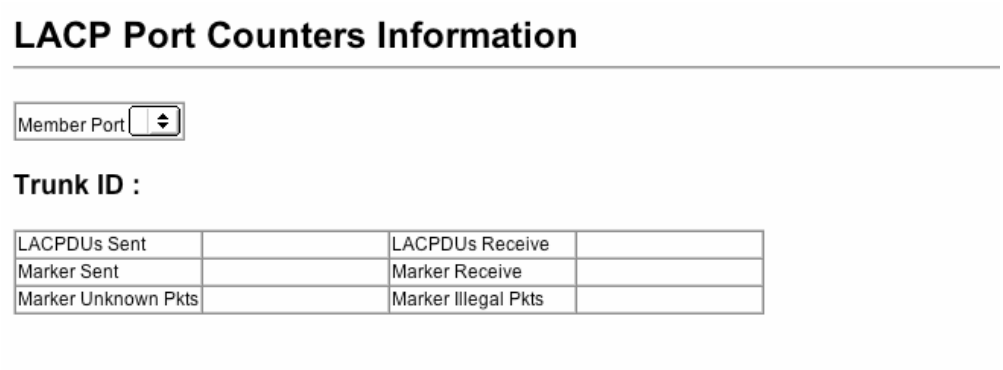
The following table shows the counter information for the LACP statistics

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

Configuring Switch Using the Web or CLI

Web

Click Port – LACP, Port Counters Information. Select a member port to display the corresponding information.



CLI

The following example displays LACP counters for port channel 1.

```
Console#show lacp 1 counters
Channel group : 1 ------------------------------------------------------------
Eth 1/ 1 --------------------------------------------------------------------
  LACPDUs Sent : 21
  LACPDUs Received : 21
  Marker Sent : 0
  Marker Received : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
.
.
.
Console#
```

7.4.3 Displaying LACP Settings and Status for the Local Side

You can display configuration settings and the operational state for the local side of an link aggregation.

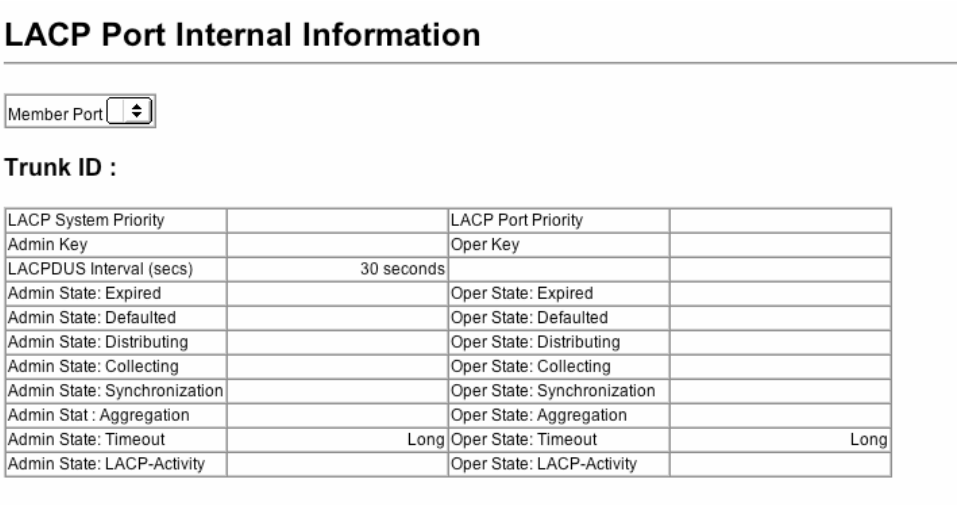
The following table describes the internal configuration information from the LACP display.

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: Expired – The actor's receive machine is in the expired state; Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. Distributing – If false, distribution of outgoing frames on this link is disabled; For example, distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. Collecting – Collection of incoming frames on this link is enabled; For example, collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. Synchronization – The System considers this link to be IN_SYNC; For example, it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted.

	Aggregation – The system considers this link to be aggregatable; For example, a potential candidate for aggregation. Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

Web

Click Port – LACP, Port Internal Information. Select a port channel to display the corresponding information.



LACP Port Internal Information

Member Port

Trunk ID :

LACP System Priority		LACP Port Priority	
Admin Key		Oper Key	
LACPDUS Interval (secs)	30 seconds		
Admin State: Expired		Oper State: Expired	
Admin State: Defaulted		Oper State: Defaulted	
Admin State: Distributing		Oper State: Distributing	
Admin State: Collecting		Oper State: Collecting	
Admin State: Synchronization		Oper State: Synchronization	
Admin Stat : Aggregation		Oper State: Aggregation	
Admin State: Timeout	Long	Oper State: Timeout	Long
Admin State: LACP-Activity		Oper State: LACP-Activity	

Configuring Switch Using the Web or CLI

CLI

The following example displays the LACP configuration settings and operational state for the local side of port channel 1.

```
Console#show lacp 1 internal
Channel group : 1
------------------------------------------------------------------------
Oper Key : 4
Admin Key : 0
Eth 1/1
------------------------------------------------------------------------
  LACPDUs Internal : 30 sec
  LACP System Priority : 32768
  LACP Port Priority : 32768
  Admin Key : 4
  Oper Key : 4
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State : distributing, collecting, synchronization, aggregation,
               long timeout, LACP-activity
Console#
```

7.4.4 Displaying LACP Settings and Status for the Remote Side

You can display configuration settings and the operational state for the remote side of an link aggregation.

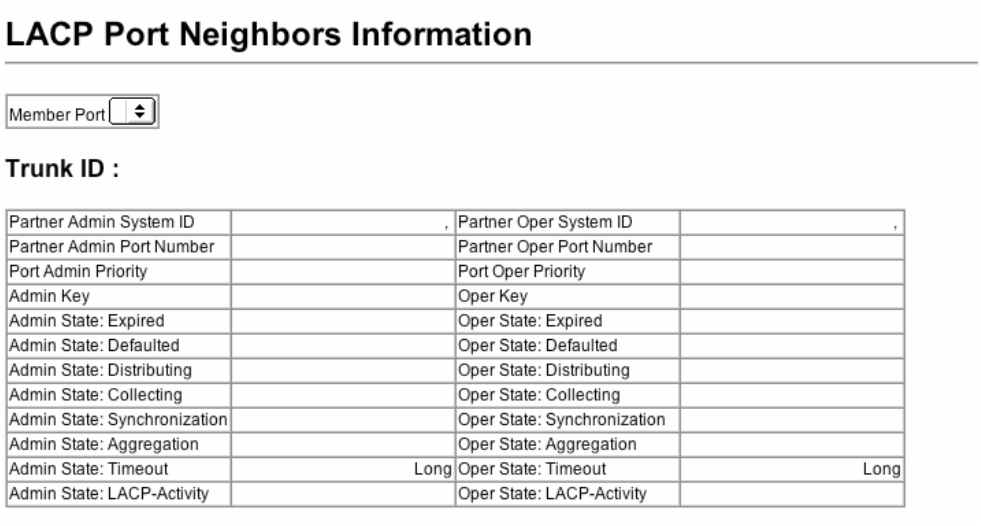
The following table lists the display information from the LACP remote setting output.

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table in section **7.4.3**.)
Oper State	Operational values of the partner's state parameters. (See preceding table in section **4.7.3**.)

Configuring Switch Using the Web or CLI

Web

Click Port – LACP, Port Neighbors Information. Select a port channel to display the corresponding information.



LACP Port Neighbors Information

Member Port

Trunk ID :

Partner Admin System ID	,	Partner Oper System ID	,
Partner Admin Port Number		Partner Oper Port Number	
Port Admin Priority		Port Oper Priority	
Admin Key		Oper Key	
Admin State: Expired		Oper State: Expired	
Admin State: Defaulted		Oper State: Defaulted	
Admin State: Distributing		Oper State: Distributing	
Admin State: Collecting		Oper State: Collecting	
Admin State: Synchronization		Oper State: Synchronization	
Admin State: Aggregation		Oper State: Aggregation	
Admin State: Timeout	Long	Oper State: Timeout	Long
Admin State: LACP-Activity		Oper State: LACP-Activity	

CLI

The following example displays the LACP configuration settings and operational state for the remote side of port channel 1.

```
Console#show lacp 1 neighbors
Channel group 1 neighbors
-------------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------------
  Partner Admin System ID : 32768, 00-00-00-00-00-00
  Partner Oper System ID : 32768, 00-00-00-00-00-01
  Partner Admin Port Number : 1
  Partner Oper Port Number : 1
  Port Admin Priority : 32768
  Port Oper Priority : 32768
  Admin Key : 0
  Oper Key : 4
  Admin State : defaulted, distributing, collecting, synchronization,
                long timeout,
  Oper State : distributing, collecting, synchronization, aggregation,
               long timeout, LACP-activity
.
.
.
Console#
```

7.5 Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

7.5.1 Guidelines

Broadcast Storm Control is enabled by default.

The default threshold is 500 packets per second.

Broadcast control does not effect IP multicast traffic.

The specified threshold applies to all ports on the switch.

Command Attributes

Port – Port number.

Type – Indicates the port type. (1000BASE-T, 1000BASE-SX, 1000BASE-LX or 100BASE-LH)

Protect Status – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)

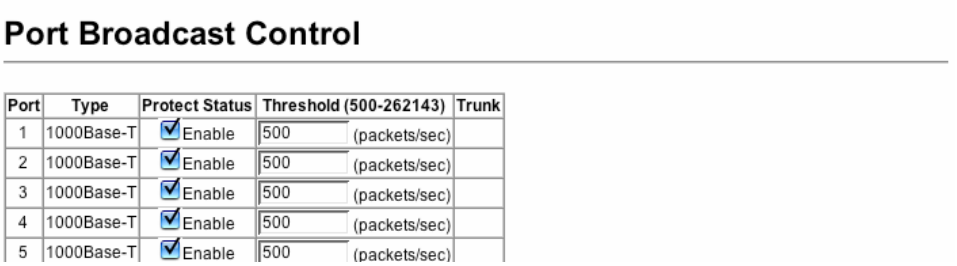
Threshold – Threshold as percentage of port bandwidth. (Range: 500-262143 packets per second; Default: 500)

Trunk – Shows if port is a trunk member.

Configuring Switch Using the Web or CLI

Web

Click Port – Port/Trunk Broadcast Control. Set the threshold and click Apply.



CLI

Specify any interface, and then enter the threshold. The following disables broadcast storm control for port 1, and then sets broadcast suppression at 600 packets per second for port 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#no switchport broadcast
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#end
Console#show interfaces switchport ethernet 1/2
Information of Eth 1/2
 Broadcast threshold: Enabled, 600 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,1000M bits per second
 Egress rate limit: disable,1000M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
```

```
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

7.6 Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

7.6.1 Guidelines

Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.

All mirror sessions have to share the same destination port.

When mirroring port traffic, the target port must be included in the same VLAN as the source port.

Command Attributes

Mirror Sessions – Displays a list of current mirror sessions.

Source Port – The port whose traffic will be monitored.

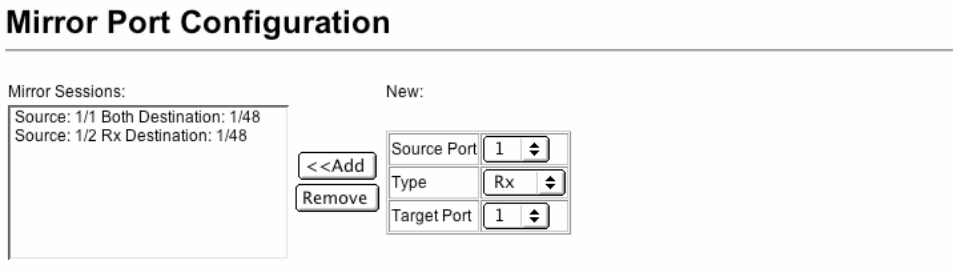
Type – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both.

Target Port – The port that duplicates (mirrors) the traffic on the source port.

Configuring Switch Using the Web or CLI

Web

Click Port – Mirror Port configuration. Specify the source port, the traffic type to be mirrored, and the monitor port, then click Add.



CLI

Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/10
Console(config-if)#port monitor ethernet 1/13
Console(config-if)#
```

7.7 Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic coming out of the switch. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command Attribute

Rate Limit – Sets the output rate limit for an interface.

Default Status – Disabled

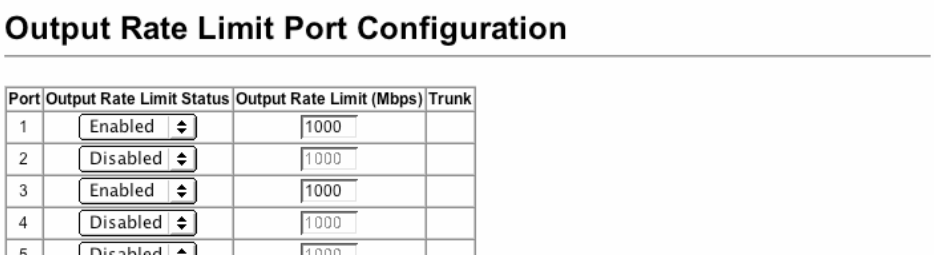
Default Rate – 1000 Mbps

Range – 1 - 1000 Mbps

Configuring Switch Using the Web or CLI

Web

Click Rate – Limit Input/Output Port/Trunk Configuration. Set the Input Rate Limit Status or Output Rate Limit Status, then set the rate limit for the individual interfaces, and click Apply.



CLI

This example sets the rate limit for input and output traffic passing through port 1 to 600 Mbps.

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 600
Console(config-if)#rate-limit output 600
Console(config-if)#
```

7.8 Showing Port Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential

problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as HP OpenView.

The following table lists the statistical values from the show port display.

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received using the interface that were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of

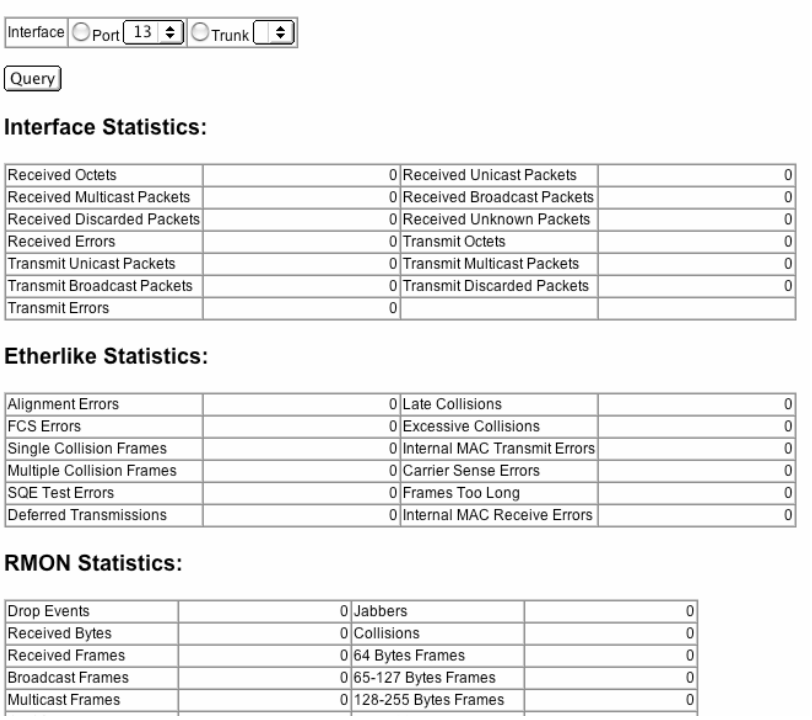
	errors.
Etherlike Statistics	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or an alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Frames	The total number of frames (bad, broadcast and multicast) received.

Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or an alignment error.
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65--1518 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Configuring Switch Using the Web or CLI

Web

Click Port – Port Statistics. Select the required interface, and click Query. You can also use the Refresh button at the bottom of the page to update the screen.


Interface
Port 13
Trunk
Query
Interface Statistics:
Received Octets 0 Received Unicast Packets 0
Received Multicast Packets 0 Received Broadcast Packets 0
Received Discarded Packets 0 Received Unknown Packets 0
Received Errors 0 Transmit Octets 0
Transmit Unicast Packets 0 Transmit Multicast Packets 0
Transmit Broadcast Packets 0 Transmit Discarded Packets 0
Transmit Errors 0
Etherlike Statistics:
Alignment Errors 0 Late Collisions 0
FCS Errors 0 Excessive Collisions 0
Single Collision Frames 0 Internal MAC Transmit Errors 0
Multiple Collision Frames 0 Carrier Sense Errors 0
SQE Test Errors 0 Frames Too Long 0
Deferred Transmissions 0 Internal MAC Receive Errors 0
RMON Statistics:
Drop Events 0 Jabbers 0
Received Bytes 0 Collisions 0
Received Frames 0 64 Bytes Frames 0
Broadcast Frames 0 65-127 Bytes Frames 0
Multicast Frames 0 128-255 Bytes Frames 0

CLI

This example shows statistics for port 13.

```
Console#show interfaces counters ethernet 1/13
Ethernet 1/13
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```

Chapter 8: Configuring Address Table Settings

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

8.1 Setting Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address is ignored and is not written to the address table.

Command Attributes

Static Address Counts (Web Only) – The number of manually configured addresses.

Current Static Address Table – Lists all the static addresses.

Interface – Port or trunk associated with the device assigned a static address.

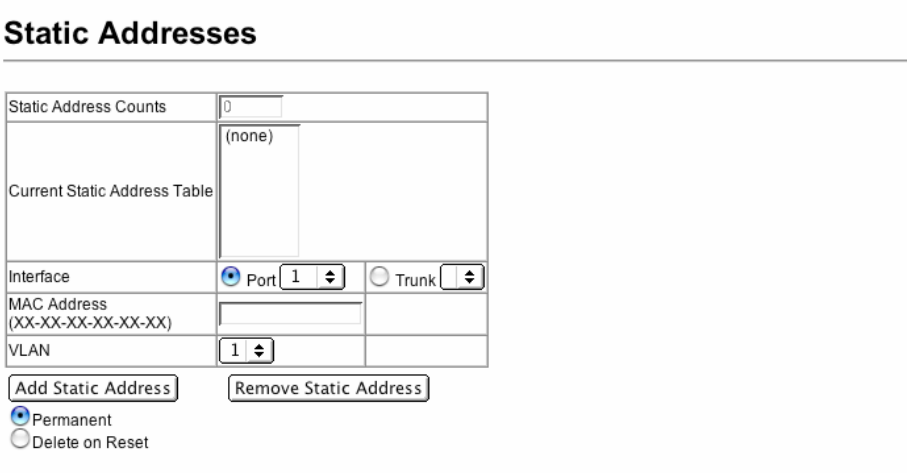
MAC Address – Physical address of a device mapped to this interface.

VLAN – ID of configured VLAN (1-4094).

Configuring Switch Using the Web or CLI

Web

Click Address Table – Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address. Then set this as a permanent address or to be deleted on reset.



CLI

This example adds an address to the static address table, but sets it to be deleted when the switch is reset.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
1/1 vlan 1 delete-on-reset
Console(config)#
```

8.2 Displaying the Dynamic Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Attributes

Interface – Indicates a port or trunk.

MAC Address – Physical address associated with this interface.

VLAN – ID of configured VLAN (1-4094).

Address Table Sort Key – You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).

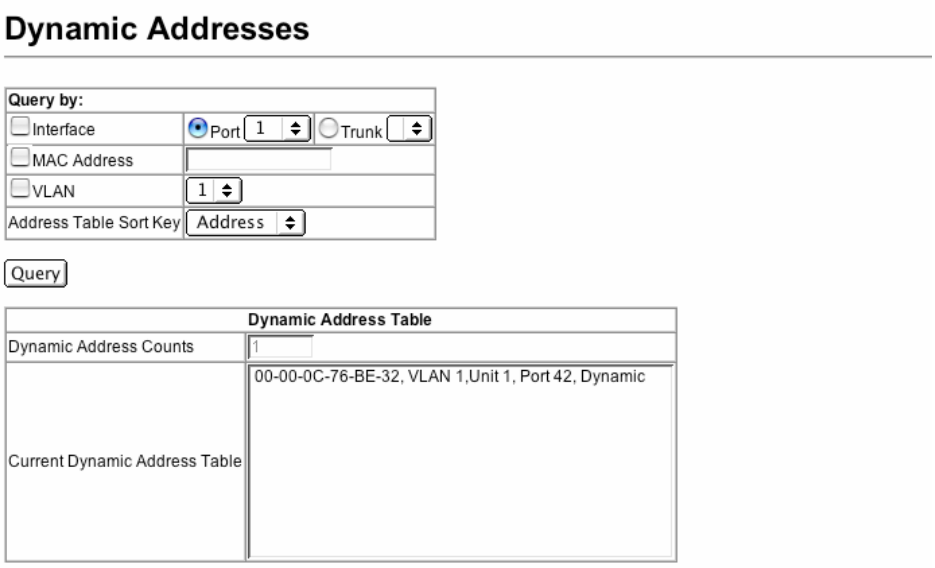
Dynamic Address Counts – The number of addresses dynamically learned.

Current Dynamic Address Table – Lists all the dynamic addresses.

Configuring Switch Using the Web or CLI

Web

Click Address Table – Dynamic Addresses. Specify the search type (For example, mark the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses, and then click Query.



CLI

This example also displays the address table entries for port 1.

```
Console#show mac-address-table interface ethernet 1/1
 Interface Mac Address       Vlan Type
```

```
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-E0-29-94-34-DE    1 Permanent
  Eth 1/ 1 00-20-9C-23-CD-60    2 Learned
Console#
```

8.3 Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

Command Attributes

Aging Status – Enables or disables the aging time.

Aging Time – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

Configuring Switch Using the Web or CLI

Web

Click Address Table – Address Aging. Specify the new aging time, click Apply.

CLI

This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table aging-time 400
Console(config)#
```

Chapter 9: Configuring Spanning Tree

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links that automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device), which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN, which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves must faster reconfiguration (For example, around one tenth of the time required by STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (an extension of RSTP) is designed to support independent spanning trees based on VLAN groups. Once you specify the VLANs to include in a Multiple Spanning Tree Instance (MSTI), the protocol automatically builds an MSTI tree to maintain connectivity between each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

9.1.1 Displaying Global Settings

You can display a summary of the current bridge STA information that applies to the entire switch using the STA Information screen.

Field Attributes

Spanning Tree State – Shows if the switch is enabled to participate in an STA-compliant network.

Bridge ID – A unique identifier for this bridge, consisting of the bridge priority and MAC address (where the address is taken from the switch system).

Max Age – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration

messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)

Hello Time – Interval (in seconds) at which the root device transmits a configuration message.

Forward Delay – The maximum time (in seconds) the root device waits before changing states (for example, discarding to learning to forwarding). This delay is required as every device must receive information about topology changes before it starts to forward frames. Each port needs time to detect conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

Designated Root – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.

Root Port – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

Root Path Cost – The path cost from the root port on this switch to the root device.

Configuration Changes – The number of times the Spanning Tree has been reconfigured.

Last Topology Change – Time since the Spanning Tree was last reconfigured.

These additional parameters are only displayed for the CLI:

Spanning tree mode – Specifies the type of spanning tree used on this switch:

- STP: Spanning Tree Protocol (IEEE 802.1D)
- RSTP: Rapid Spanning Tree (IEEE 802.1w)
- MSTP: Multiple Spanning Tree (IEEE 802.1s)

Instance – Instance identifier of this spanning tree. (This is always 0 for the CIST.)

Vlans configuration – VLANs assigned to the CIST.

Priority – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device.

Root Hello Time – Interval (in seconds) at which this device transmits a configuration message.

Root Maximum Age – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)

Root Forward Delay – The maximum time (in seconds) this device will wait before changing states (For example, discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

Root Hold Time – The interval (in seconds) during which no more than two bridge configuration protocol data units shall be transmitted by this node.

Max hops – The max number of hop counts for the MST region.

Remaining hops – The remaining number of hop counts for the MST instance.

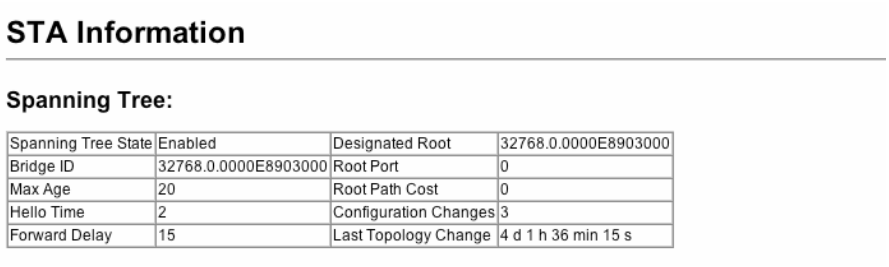
Transmission limit – The minimum interval between the transmissions of consecutive RSTP/MSTP BPDUs.

Path Cost Method – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

Configuring Switch Using the Web or CLI

Web

Click Spanning Tree – STA, Information.



STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0.0000E8903000
Bridge ID	32768.0.0000E8903000	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	3
Forward Delay	15	Last Topology Change	4 d 1 h 36 min 15 s

CLI

This command displays global STA settings, followed by settings for each port.

```
Console#show spanning-tree
Spanning-tree information
----------------------------------------------------------------
 Spanning tree mode               :MSTP
 Spanning tree enable/disable     :enable
 Instance                         :0
 Vlans configuration              :1-4094
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Max hops                         :20
 Remaining hops                   :20
 Designated Root                  :32768.0.0000ABCD0000
 Current root port                :1
 Current root cost                :200000
 Number of topology changes       :1
 Last topology changes time (sec.):13380
 Transmission limit               :3
 Path Cost Method                 :long
```

Note: The current root port and current root cost display as zero when this device is not connected to the network.

Chapter 10: Configuring VLAN

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

10.1 Assigning Ports to VLANs

Before enabling VLANs for the switch, assign each port to the VLAN group(s) where it participates. By default, all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Use GVRP, either manually or dynamically, to assign ports on other VLAN-aware network devices on a path that carries this traffic to the same VLAN(s). If you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices or the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags are stripped off before passing it on to any end host that does not support VLAN tagging.

VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). If the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. If you implement VLANs that do not overlap, but still need to communicate, you can connect them by using a Layer-3 router or switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other

VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. Use IEEE 802.3 tagged VLANs with GVRP to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system where the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on end station requests.

To implement GVRP in a network, add the host devices to the required VLANs (using the operating system or other application software), so the VLANs can be propagated onto the network. For both edge switches attached directly to these hosts and core switches in the network, enable GVRP on the links between these devices. Also, determine security boundaries in the network and disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

Note: Host devices that do not support GVRP should be configured as static or untagged VLANs for the switch ports connected to these devices (see section **10.1.6 Adding Static Members to VLANs (VLAN Index)**. You can still enable GVRP on these edge switches, as well as on the core switches in the network.

10.1.1 Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. To participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it passes this frame onto the VLAN(s) indicated by the frame tag. When this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

10.1.2 Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information and to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration and to support VLANs that extend beyond the local switch. (Default: Disabled)

Configuring Switch Using the Web or CLI

Web

Click VLAN – 802.1Q VLAN, GVRP Status. Enable or disable GVRP, and click Apply.

CLI

This example enables GVRP for the switch.

```
Console(config)#bridge-ext gvrp
Console(config)#
```

10.1.3 Displaying Basic VLAN Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Field Attributes

VLAN Version Number (Web Only) – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.

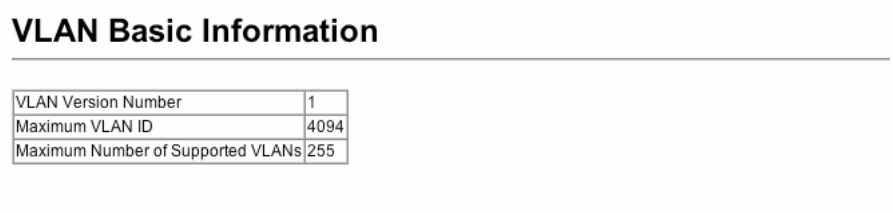
Maximum VLAN ID – Maximum VLAN ID recognized by this switch.

Maximum Number of Supported VLANs – Maximum number of VLANs that can be configured on this switch.

Configuring Switch Using the Web or CLI

Web

Click VLAN – 802.1Q VLAN, Basic Information.



CLI

Enter the following command.

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

10.1.4 Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. If you want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes (Web)

VLAN ID – ID of configured VLAN (1-4094).

Up Time at Creation – Time this VLAN was created (For example, System Up Time).

Status – Shows how this VLAN was added to the switch.

- Dynamic GVRP: Automatically learned via GVRP.
- Permanent: Added as a static entry.

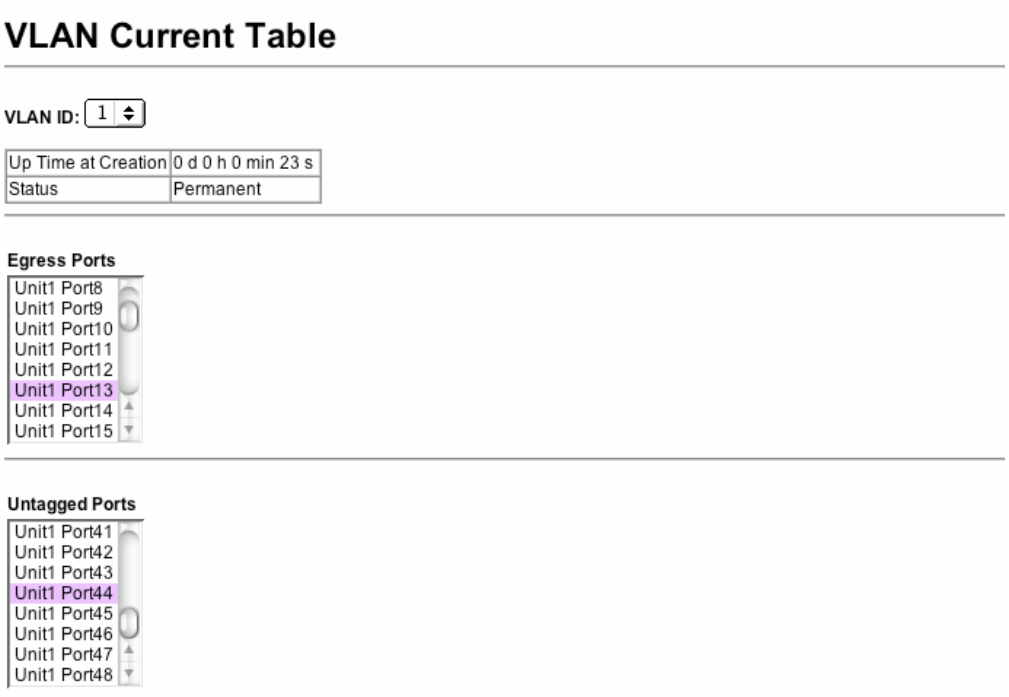
Egress Ports – Shows all the VLAN port members.

Untagged Ports – Shows the untagged VLAN port members.

Configuring Switch Using the Web or CLI

Web

Click VLAN – 802.1Q VLAN, Current Table. Select any ID from the scroll-down list.



Command Attributes (CLI)

VLAN – ID of configured VLAN (1-4094, no leading zeroes).

Type – Shows how this VLAN was added to the switch.

- Dynamic: Automatically learned via GVRP.
- Static: Added as a static entry.

Name – Name of the VLAN (1 to 32 characters).

Status – Shows if this VLAN is enabled or disabled.

- Active: VLAN is operational.
- Suspend: VLAN is suspended; For example, does not pass packets.

Ports / Channel groups – Shows the VLAN interface members.

CLI

Current VLAN information can be displayed with the following command.

```
Console#show vlan id
VLAN Type    Name         Status   Ports/Channel groups
---- ------- ------------ ------   -----------------------------------
1    Static  DefaultVlan  Active Eth1/1  Eth1/2
Console#
```

10.1.5 Creating VLANs

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Command Attributes

Current – List all the current VLAN groups created for this system. Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

New – Specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)

VLAN ID – ID of configured VLAN (1-4094, no leading zeroes).

VLAN Name – Name of the VLAN (1 to 32 characters).

Status (Web) – Enable or disable the specified VLAN.

- Enable: VLAN is operational.
- Disable: VLAN is suspended; For example, does not pass packets.

State (CLI) – Enable or disable the specified VLAN.

- Active: VLAN is operational.
- Suspend: VLAN is suspended; For example, does not pass packets.

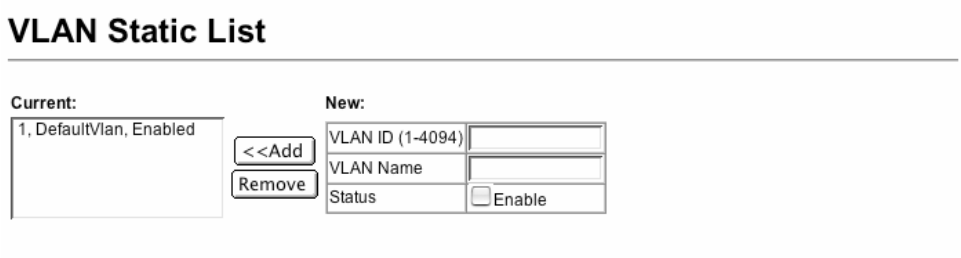
Add – Add a new VLAN group to the current list.

Remove – Remove a VLAN group from the current list. If any port is assigned to this group as untagged, it is reassigned to VLAN group 1 as untagged.

Configuring Switch Using the Web or CLI

Web

Click VLAN – 802.1Q VLAN, Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.



CLI

This example creates a new VLAN.

```
Console(config)#vlan database
Console(config-vlan)#vlan 2 name R&D media ethernet state active
Console(config-vlan)#end
Console#show vlan
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- ----------------------------------
   1  Static      DefaultVlan    Active Eth1/ 1 Eth1/ 2
   2  Static              R&D    Active Eth1/ 3 Eth1/ 4
   3  Static                     Active Eth1/ 5 Eth1/ 6
   4  Static                     Active Eth1/ 7 Eth1/ 8
   5  Static                     Active Eth1/ 9 Eth1/10
   6  Static                     Active Eth1/11 Eth1/12
   7  Static                     Active Eth1/13 Eth1/14
   8  Static                     Active Eth1/15 Eth1/16
.
.
.

Console(config-vlan)#
```

10.1.6 Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. You can also configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

Note: You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index (**10.1.7**). This configuration page can only add ports to a VLAN as tagged members.

VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under section **10.1.8 Configuring VLAN Behavior for Interfaces**.

Command Attributes

VLAN – ID of configured VLAN (1-4094, no leading zeroes).

Name – Name of the VLAN (1 to 32 characters).

Status – Enables or disables the specified VLAN.

- Enable: VLAN is operational.
- Disable: VLAN is suspended; For example, does not pass packets.

Port – Port identifier.

Trunk – Trunk identifier.

Membership Type – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:

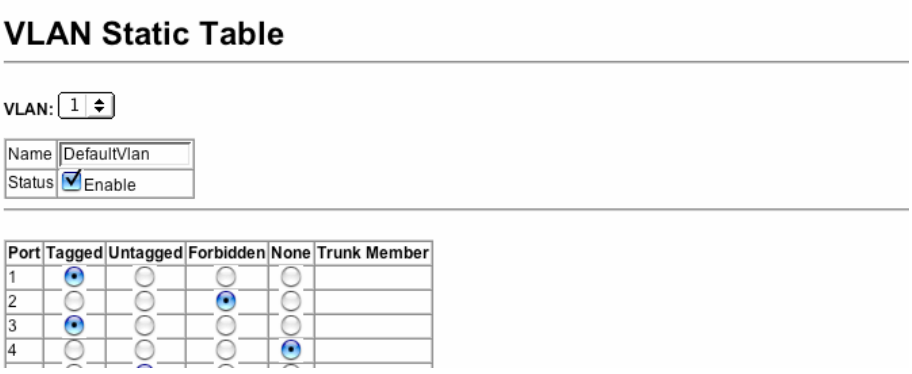
- Tagged: Interface is a member of the VLAN. All packets transmitted by the port carries a tag with VLAN or CoS information.
- Untagged: Interface is a member of the VLAN. All packets transmitted by the port does not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
- Forbidden: Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see “Automatic VLAN Registration” in section **10.1 Assigning VLAN Ports**.
- None: Interface is not a member of the VLAN. Packets associated with this VLAN is not transmitted by the interface.

Trunk Member – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Configuring Switch Using the Web or CLI

Web

Click VLAN – 802.1Q VLAN, Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.



CLI

The following example adds tagged and untagged ports to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 2 tagged     4
Console(config-if)#exit
```

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
```

10.1.7 Adding Static Members to VLANs (Port Index)

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface as a tagged member.

Command Attributes

Interface – Port or trunk identifier.

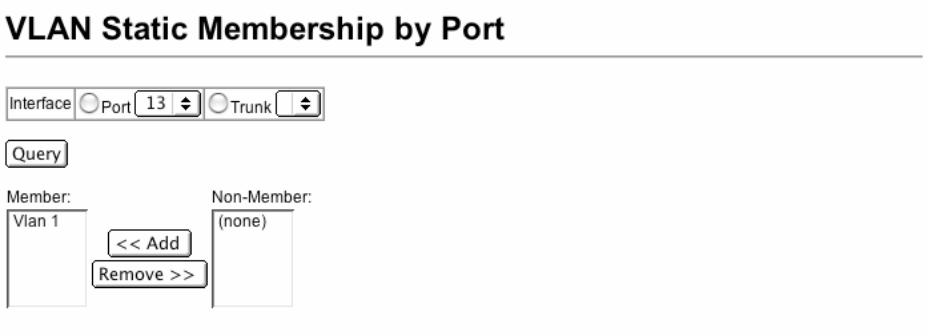
Member – VLANs for which the selected interface is a tagged member.

Non-Member – VLANs for which the selected interface is not a tagged member.

Configuring Switch Using the Web or CLI

Web

Open VLAN – 802.1Q VLAN, Static Membership. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.



CLI

This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport allowed vlan add 1 tagged
Console(config-if)#switchport allowed vlan remove 2
```

10.1.8 Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP timers.

Usage Guidelines

GVRP – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information to automatically register VLAN members on interfaces across the network.

GARP – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration.

Command Attributes

PVID – VLAN ID assigned to untagged frames received on the interface. (Default: 1)

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.

Acceptable Frame Type – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)

Ingress Filtering – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)

- Ingress filtering only affects tagged frames.

- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).

- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.

- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. They do affect VLAN dependent BPDU frames, such as GMRP.

GVRP Status – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect. (See section **2.4.10 Displaying Bridge Extension Capabilities**) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)

GARP Join Timer – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20) (Timer settings: 2 x (join timer) < leave timer < leaveAll timer)

GARP Leave Timer – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60) (Timer settings: 2 x (join timer) < leave timer < leaveAll timer)

GARP LeaveAll Timer – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000) (Timer settings: 2 x (join timer) < leave timer < leaveAll timer)

Mode – Indicates VLAN membership mode for an interface. (Default: 1Q Trunk)

- 1Q Trunk – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging

to the port's default VLAN (For example, associated with the PVID) are also transmitted as tagged frames.

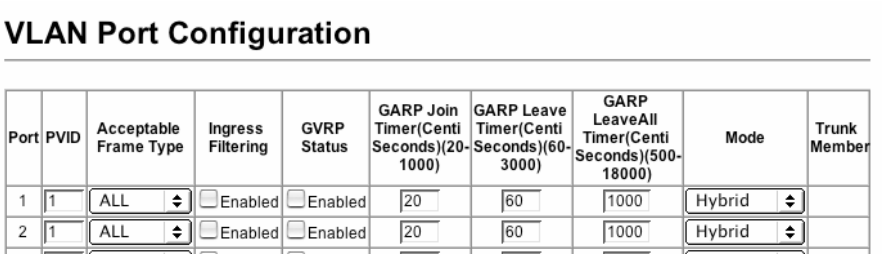
- Hybrid – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

Trunk Member – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Configuring Switch Using the Web or CLI

Web

Click VLAN – 802.1Q VLAN, Port Configuration or VLAN Trunk Configuration. Fill in the required settings for each interface, click Apply.



CLI

This example sets port 3 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to hybrid.

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport native vlan 3
Console(config-if)#switchport gvrp
Console(config-if)#garp timer join 20
Console(config-if)#garp timer leave 90
Console(config-if)#garp timer leaveall 2000
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

10.2 Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports. (Private VLANs and normal VLANs can exist simultaneously within the same switch.)

10.2.1 Enabling Private VLANs

Use the Private VLAN Status page to enable/disable the Private VLAN function. (Default: Disabled)

Configuring Switch Using the Web or CLI

Web

Click VLAN – Private VLAN, Status. Select Enable or Disable from the scroll-down box, and click Apply.

CLI

This example enables private VLANs.

```
Console(config)#pvlan
Console(config)#
```

10.2.2 Configuring Uplink and Downlink Ports

Use the Private VLAN Link Status page to set ports as downlink or uplink ports. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

Configuring Switch Using the Web or CLI

Web

Click VLAN – Private VLAN, Link Status. Mark the ports that will serve as uplinks and downlinks for the private VLAN, then click Apply.

CLI

This configures ports 3 and 4 as uplinks and ports 5 and 6 as downlinks.

```
Console(config)#pvlan uplink ethernet 1/3-4 downlink ethernet 1/5-6
Console(config)#
```

10.3 Configuring Protocol-Based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Usage Guidelines

To configure protocol-based VLANs, follow these steps:

1. Configure VLAN groups for the protocols you want to use (section **10.1.5**). You should configure a separate VLAN for each major protocol running on your network. Do not add port members at this time.

2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Protocol VLAN Configuration page.

3. Then map the protocol for each interface to the appropriate VLAN using the Protocol VLAN Port Configuration page.

10.3.1 Configuring Protocol Groups

Create a protocol group for one or more protocols.

Command Attributes

Protocol Group ID – Group identifier of this protocol group. (Range: 1-2147483647)

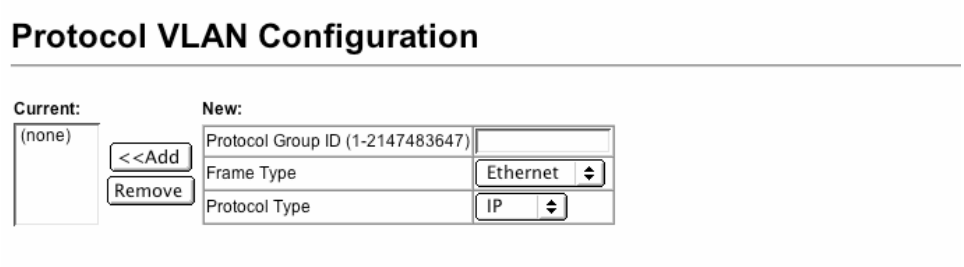
Frame Type – Frame type used by this protocol. (Options: Ethernet, RFC_1042, LLC_other)

Protocol Type – The only option for the LLC_other frame type is IPX_raw. The options for all other frames types include: IP, ARP, RARP.

Configuring Switch Using the Web or CLI

Web

Click VLAN – Protocol VLAN, Configuration. Enter a protocol group ID, frame type and protocol type, then click Apply.



CLI

The following creates protocol group 1, and then specifies Ethernet frames with IP and ARP protocol types.

```
Console(config)#protocol-vlan protocol-group 1 add frame_type ethernet
protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame_type ethernet
protocol-type arp
Console(config)#
```

10.3.2 Mapping Protocols to VLANs

Map a protocol group to a VLAN for each interface that will participate in the group.

Usage Guidelines

When creating a protocol-based VLAN, only assign interfaces using this configuration screen. If you assign interfaces using any of the other VLAN commands such as VLAN Static Table (section **10.1.6 Adding Static Members to VLANs (VLAN Index)**.) or VLAN Static Membership (in section **10.1.7 Adding Static Members to VLANs (Port Index**), these interfaces will admit traffic of any protocol type into the associated VLAN.

When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:

- If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
- If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
- If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Command Attributes

Interface – Port or trunk identifier.

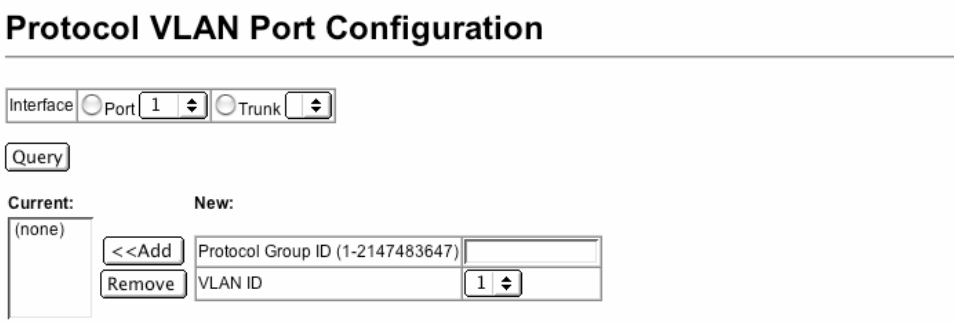
Protocol Group ID – Group identifier of this protocol group. (Range: 1-2147483647)

VLAN ID – VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

Configuring Switch Using the Web or CLI

Web

Click VLAN – Protocol VLAN, Port Configuration. Select a port or trunk, enter a protocol group ID, the corresponding VLAN ID, and click Apply.



CLI

The following maps the traffic entering Port 1, which matches the protocol type specified in protocol group 1 to VLAN 3.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan
Console(config-if)#
```

Chapter 11: Configuring Packet Priority

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

11.1 Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Follow these guidelines:

- This switch provides four priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (for example, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

Default Priority (CLI Only) – The priority that is assigned to untagged frames received on the specified interface. (Range: 0 - 7, Default: 0)

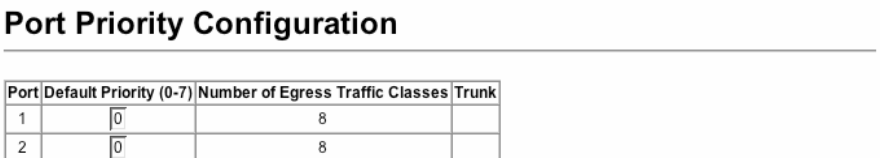
Number of Egress Traffic Classes – The number of queue buffers provided for each port.

The information is displayed as "Priority for untagged traffic."

Configuring Switch Using the Web or CLI

Web

Click Priority – Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.



CLI

This example assigns a default priority of 5 to port 3.

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
Console(config-if)#end
```

```
Console#show interfaces switchport ethernet 1/5
Information of Eth 1/3
 Broadcast threshold: Enabled, 500 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,1000M bits per second
 Egress rate limit: disable,1000M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 5
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

11.2 Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict or Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

The following table gives information for mapping CoS values to egress queues.

Queue	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Priority	2	0	1	3	4	5	6	7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. You can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

Priority Level	**Traffic Type**
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

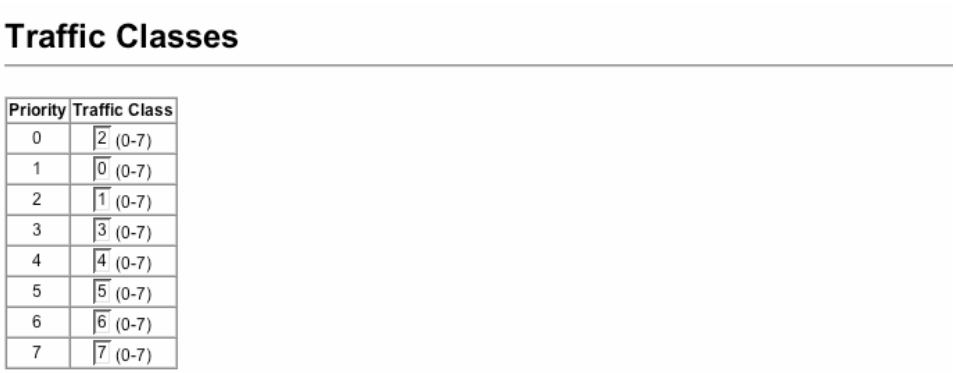
Priority – CoS value. (Range: 0-7, where 7 is the highest priority)

Traffic Class (CLI show queue)– Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

Configuring Switch Using the Web or CLI

Web

Click Priority – Traffic Classes. Mark an interface and click Select to display the current mapping of CoS values to output queues. Assign priorities to the traffic classes (for example, output queues) for the selected interface, then click Apply.



CLI

The following example shows how to change the CoS assignments to a one-to-one mapping.

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#end
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value     : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
console#
```

Mapping specific values for CoS priorities is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

11.3 Selecting the Queue Mode

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Command Attributes

WRR - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 through 7 respectively. (This is the default selection.)

Strict - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

Configuring Switch Using the Web or CLI

Web

Click Priority – Queue Mode. Select Strict or WRR, then click Apply.

CLI

The following sets the queue mode to strict priority service mode.

```
Console(config)#queue mode strict
Console(config)#exit
Console#show queue mode

Queue mode: strict
Console#
```

11.4 Setting the Service Weight for Traffic Classes

This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in section **11.2 Mapping CoS Values to Egress Queues**, the traffic classes are mapped to one of the eight egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes

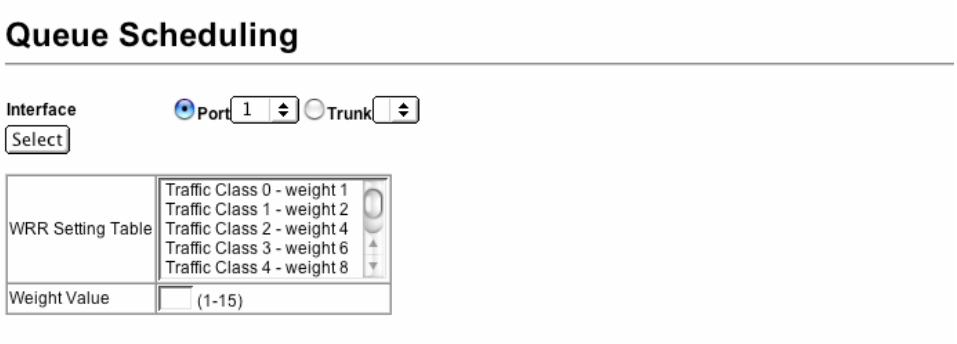
WRR Setting Table* – Displays a list of weights for each traffic class (CLI shows Queue ID).

Weight Value – Set a new weight for the selected traffic class. (Range: 1-15)

Configuring Switch Using the Web or CLI

Web

Click Priority – Queue Scheduling. Select the interface, highlight a traffic class (for example, output queue), enter a weight, then click Apply.



CLI

The following example shows how to assign WRR weights to each of the priority queues.

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue bandwidth 1 3 5 7 9 11 13 15 4-189
Console(config-if)#end
Console#show queue bandwidth
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
    0         1
    1         3
    2         5
    3         7
    4         9
    5         11
    6         13
    7         15
Information of Eth 1/2
 Queue ID  Weight
.
.
.
```

11.4.1 Mapping Layer 3/4 Priorities to CoS Values

This switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet or the number of the TCP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

The precedence for priority mapping is IP Precedence or DSCP Priority, and then Default Port Priority.

IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.

11.5 Selecting IP Precedence/DSCP Priority

The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes

Disabled – Disables both priority services. (This is the default setting.)

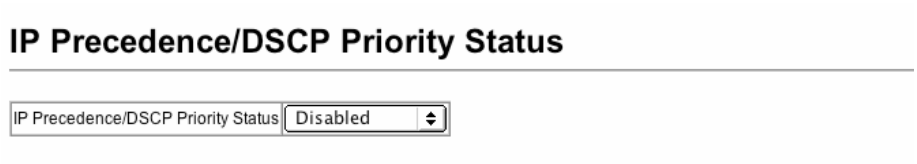
IP Precedence – Maps layer 3/4 priorities using IP Precedence.

IP DSCP – Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

Configuring Switch Using the Web or CLI

Web

Click Priority – IP Precedence/DSCP Priority Status. Select Disabled, IP Precedence or IP DSCP from the scroll-down menu.



CLI

The following example enables IP Precedence service on the switch.

```
Console(config)#map ip precedence
Console(config)#
```

11.5.1 Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (For example, Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

Priority Level	Traffic Type	Priority Level	Traffic Type
7	Network Control	3	Flash
6	Internetwork Control	2	Immediate
5	Critical	1	Priority
4	Flash Override	0	Routine

Command Attributes

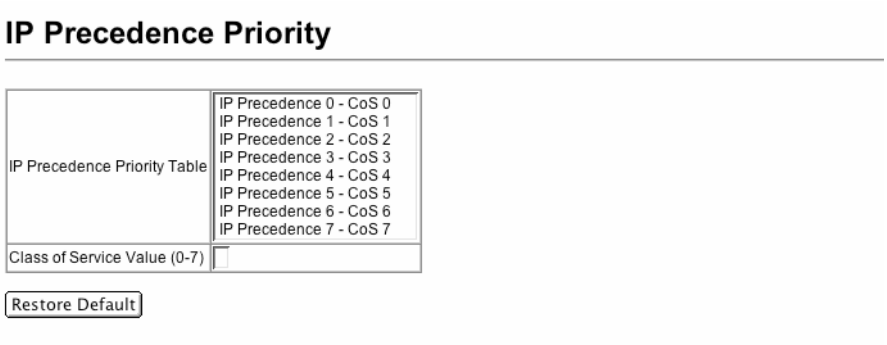
IP Precedence Priority Table – Shows the IP Precedence to CoS map.

Class of Service Value – Maps a CoS value to the selected IP Precedence value. Note that “0” represents low priority and “**7**” represent high priority.

Configuring Switch Using the Web or CLI

Web

Click Priority – IP Precedence Priority. Select an entry from the IP Precedence Priority Table, enter a value in the Class of Service Value field, and then click Apply.


IP Precedence Priority
IP Precedence Priority Table
IP Precedence 0 - CoS 0
IP Precedence 1 - CoS 1
IP Precedence 2 - CoS 2
IP Precedence 3 - CoS 3
IP Precedence 4 - CoS 4
IP Precedence 5 - CoS 5
IP Precedence 6 - CoS 6
IP Precedence 7 - CoS 7
Class of Service Value (0-7)
Restore Default

CLI

The following example globally enables IP Precedence service on the switch, maps IP Precedence value 1 to CoS value 0 (on port 1), and then displays the IP Precedence settings.

```
Console(config)#map ip precedence
Console(config)#interface ethernet 1/1
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#end
Console#show map ip precedence ethernet 1/1
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 1          0   0
  Eth 1/ 1          1   0
  Eth 1/ 1          2   2
  Eth 1/ 1          3   3
  Eth 1/ 1          4   4
  Eth 1/ 1          5   5
  Eth 1/ 1          6   6
  Eth 1/ 1          7   7
Console#
```

Mapping specific values for IP Precedence is implemented as an interface configuration command, and any changes apply to the all interfaces on the switch.

11.5.2 Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

DSCP Priority Table – Shows the DSCP Priority to CoS map.

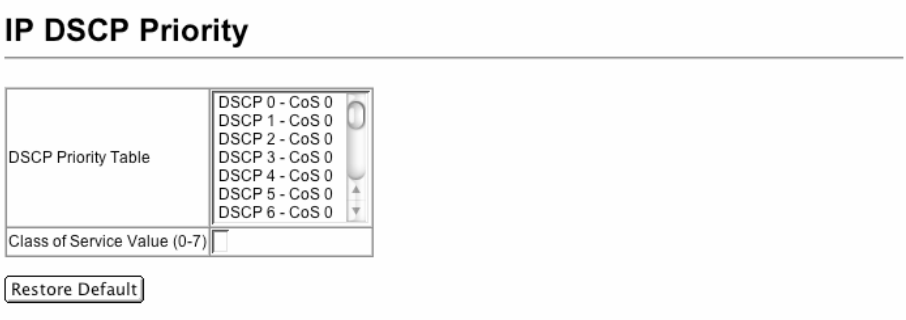
Class of Service Value – Maps a CoS value to the selected DSCP Priority value. Note that “0” represents low priority and “7” represent high priority.

Note: IP DSCP settings apply to all interfaces.

Configuring Switch Using the Web or CLI

Web

Click Priority – IP DSCP Priority. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click Apply.


IP DSCP Priority
DSCP Priority Table
DSCP 0 - CoS 0
DSCP 1 - CoS 0
DSCP 2 - CoS 0
DSCP 3 - CoS 0
DSCP 4 - CoS 0
DSCP 5 - CoS 0
DSCP 6 - CoS 0
Class of Service Value (0-7)
Restore Default

CLI

The following example globally enables DSCP Priority service on the switch, maps DSCP value 0 to CoS value 1 (on port 1), and then displays the DSCP Priority settings.

```
Console(config)#map ip dscp
Console(config)#interface ethernet 1/1
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#end
Console#show map ip dscp ethernet 1/1
DSCP mapping status: enabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
.
.
.
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

11.5.3 Mapping IP Port Priority

You can also map network applications to Class of Service values based on the IP port number (For example, TCP/UDP port number) in the frame header. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

Command Attributes

IP Port Priority Status – Enables or disables the IP port priority. (Default: Disabled)

Interface – Selects the port or trunk interface to which the settings apply.

IP Port Priority Table – Shows the IP port to CoS map.

IP Port Number (TCP/UDP) – Set a new IP port number.

Class of Service Value – Sets a CoS value for a new IP port. Note that “0” represents low priority and “7” represents high priority.

Note: IP Port Priority settings apply to all interfaces.

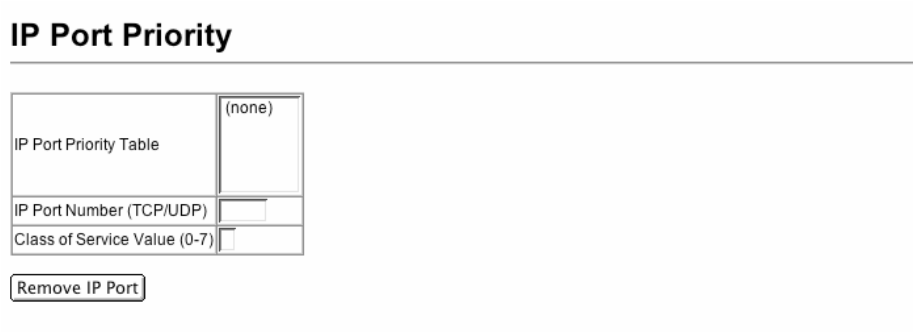
Configuring Switch Using the Web or CLI

Web

Click Priority – IP Port Priority Status. Set IP Port Priority Status to Enabled.

Web

Click Priority–IP Port Priority. Enter the IP port number for a network application in the IP Port Number box and the new CoS values in the Class of Service box, and then click Apply.



Mapping specific values for IP Precedence is implemented as an interface configuration command, and any changes apply to the all interfaces on the switch.

CLI

The following example globally enables IP Port Priority service on the switch, maps HTTP traffic on port 5 to CoS value 0, and then displays all the IP Port Priority settings for that port.

```
Console(config)#map ip port
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#end
Console#show map ip port ethernet 1/5
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

11.6 Mapping CoS Values to ACLs

Use the ACL CoS Mapping page to set the output queue for packets matching an ACL rule as shown in the following table. Note that the specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. For information on mapping the CoS values to output queues, see section **2.10 Mapping CoS Values to Egress Queues.**

Priority	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Queue	1	2	0	3	4	5	6	7

11.6.1 Guidelines

You must configure an ACL mask before you can map CoS values to the rule.

Command Attributes

Port – Port identifier.

Name – Name of ACL. For information on configuring ACLs, see section **6.7 Configuring Access Control Lists**.

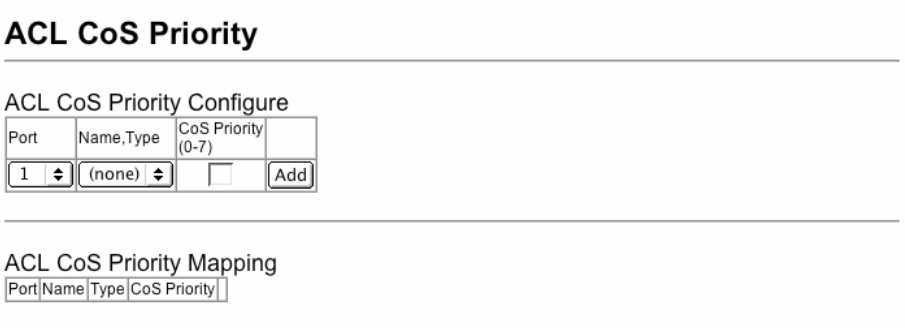
Type – Type of ACL (IP or MAC).

CoS Priority – CoS value used for packets matching an IP ACL rule. (Range: 0-7)

Configuring Switch Using the Web or CLI

Web

Click Priority – ACL CoS Priority. Enable mapping for any port, select an ACL from the scroll-down list, then click Apply.



CLI

This example assigns a CoS value of zero to packets matching rules within the specified ACL on port 24.

```
Console(config)#interface ethernet 1/24
Console(config-if)#map access-list ip bill cos 0
Console(config-if)#
```

11.7 Changing Priorities Based on ACL Rules

Change traffic priorities for frames matching the defined ACL rule. (This is the ACL packet marking feature.) This switch can change the IEEE 802.1p priority, IP Precedence, or DSCP Priority of IP frames; or change the IEEE 802.1p priority of Layer 2 frames. Use the no form to remove the ACL marker.

11.7.1 Guidelines

You must configure an ACL mask before you can change priorities based on a rule.

Traffic priorities may be included in the IEEE 802.1p priority tag. This tag is also incorporated as part of the overall IEEE 802.1Q VLAN tag. The 802.1p priority may be set for either Layer 2 or IP frames.

The IP frame header also includes priority bits in the Type of Service (ToS) octet. The Type of Service octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. Note that the IP frame header can include either the IP Precedence or the DSCP priority type.

The precedence for priority mapping by this switch is IP Precedence or DSCP Priority, and then 802.1p priority.

Command Attributes

Port – Port identifier.

Name – Name of ACL. For information on configuring ACLs, see section **6.7 Configuring Access Control Lists**.

Type – Type of ACL (IP or MAC).

Precedence – IP Precedence value. (Range: 0-7)

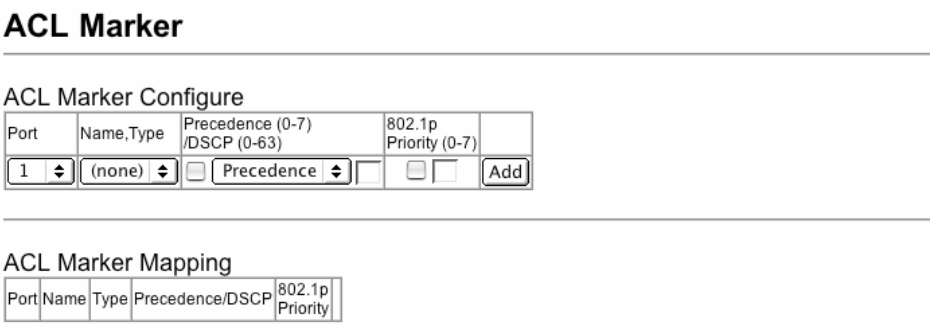
DSCP – Differentiated Services Code Point value. (Range: 0-63)

802.1p Priority – Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest priority)

Configuring Switch Using the Web or CLI

Web

Click Priority – **ACL Marker**. Select a port and an ACL rule. To specify a ToS priority, mark the Precedence/DSCP check box, select Precedence or DSCP from the scroll-down box, and enter a priority. To specify an 802.1p priority, mark the 802.1p Priority check box, and enter a priority. Then click Add.



CLI

This example changes the DSCP priority for packets matching an IP ACL rule, and the 802.1p priority for packets matching a MAC ACL rule.

```
Console(config)#interface ethernet 1/1
Console(config-if)#match access-list ip bill set dscp 0
Console(config-if)#match access-list mac mike set priority 0
Console(config-if)#end
Console#show marking
Interface ethernet 1/1
 match access-list IP bill set DSCP 0
 match access-list MAC a set priority 0
```

```
Console#
```

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

Chapter 12: Layer 2 IGMP (Snooping and Query)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and Query (section **12.1.1 Configuring IGMP Snooping and Query Parameters**) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports that need to forward multicast traffic.

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (For example, a multicast router/switch) connected over the network to an interface on your switch (section **12.1.4**). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (section **12.1.5**).

12.1 IGMP Multicast Filtering

Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts that subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. This procedure is called multicast filtering.

12.1.1 Configuring IGMP Snooping and Query Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Follow these guidelines:

- IGMP Snooping – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

- IGMP Querier – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

IGMP Status — When enabled, the switch monitors network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Enabled)

Act as IGMP Querier — When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Enabled)

IGMP Query Count — Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10, Default: 2)

IGMP Query Interval — Sets the frequency at which the switch sends IGMP host-query messages. (Range: 60-125 seconds, Default: 125)

IGMP Report Delay — Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 5-30 seconds, Default: 10)

IGMP Query Timeout — The time the switch waits after the previous querier stops before it considers the router port (For example, the interface which had been receiving query packets) to have expired. (Range: 300-500 seconds, Default: 300)

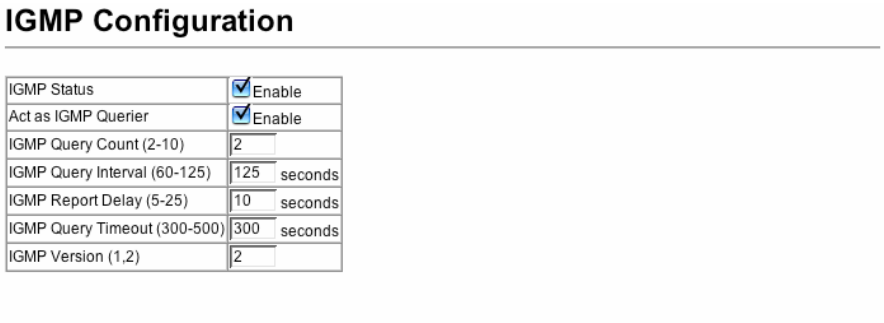
IGMP Version — Sets the protocol version for compatibility with other devices on the network. (Range: 1-2; Default: 2)

Notes: All systems on the subnet must support the same version. Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.

Configuring Switch Using the Web or CLI

Web

Click IGMP Snooping–IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)



CLI

This example modifies the settings for multicast filtering, and then displays the current status.

```
Console(config)#ip igmp snooping
Console(config)#ip igmp snooping querier
Console(config)#ip igmp snooping query-count 10
Console(config)#ip igmp snooping query-interval 100
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#ip igmp snooping version 2
Console(config)#exit
Console#show ip igmp snooping
 Service status          : Enabled
 Querier status          : Enabled
 Query count             : 10
```

```
 Query interval          : 100 sec
 Query max response time : 20 sec
 Router port expire time : 300 sec
 IGMP snooping version   : Version 2
Console#
```

12.1.2 Displaying Interfaces Attached to a Multicast Router

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Command Attributes

VLAN ID – ID of configured VLAN (1-4094).

Multicast Router List – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

Configuring Switch Using the Web or CLI

Web

Click IGMP Snooping – Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.

CLI

This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1           Eth 1/11 Static
console#
```

12.1.3 Specifying Static Interfaces for a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

Interface – Activates the Port or Trunk scroll down list.

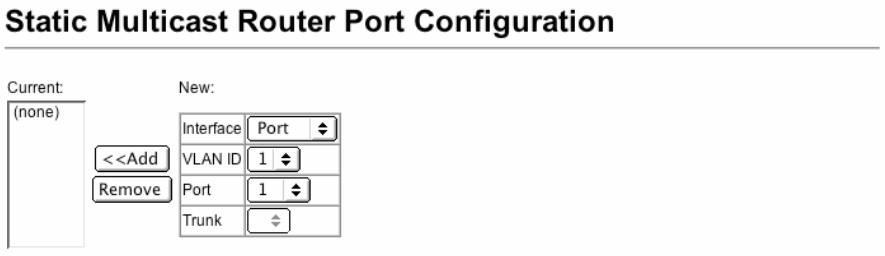
VLAN ID – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.

Port or Trunk – Specifies the interface attached to a multicast router.

Configuring Switch Using the Web or CLI

Web

Click IGMP Snooping–Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLANs forwarded all the corresponding multicast traffic, and then click Add. After you have finished adding interfaces to the list, click Apply.



CLI

This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1           Eth 1/11  Static
Console#
```

12.1.4 Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast service.

Command Attributes

VLAN ID – Selects the VLAN for which to display port members.

Multicast IP Address – The IP address for a specific multicast service.

Multicast Group Port List – Shows the interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service.

Configuring the Switch Using the Web or CLI

Web

Click IGMP Snooping – IP Multicast Registration Table. Select a VLAN ID and the IP address for a multicast service from the scroll-down lists. The switch will display all the interfaces that are propagating this multicast service.

CLI

This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The Type field shows if this entry was learned dynamically or was statically configured.

```
Console#show mac-address-table multicast vlan 1
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

12.1.5 Assigning Ports to Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in section **12.1.1 Configuring IGMP Snooping and Query Parameters**. For certain applications that require tighter control, you may need to statically configure a multicast service on the switch. First, add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Follow these guidelines.

Static multicast addresses are never aged out.

When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attribute

Interface – Activates the Port or Trunk scroll down list.

VLAN ID – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.

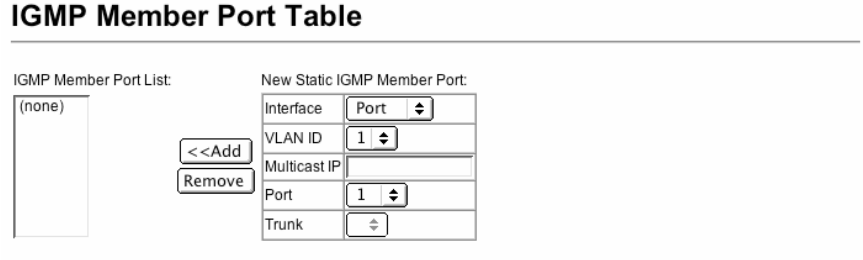
Multicast IP – The IP address for a specific multicast service

Port or Trunk – Specifies the interface attached to a multicast router/switch.

Configuring the Switch Using the Web or CLI

Web

Click IGMP Snooping – IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and click Add. After you have completed adding ports to the member list, click Apply.



CLI

This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12
ethernet 1/12
Console(config)#exit
Console#show mac-address-table multicast vlan 1
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

Chapter 13: Configuring Domain Name Service

The Domain Naming System (DNS) service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.

You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

13.1 General DNS Server Parameters

Follow these guidelines.

To enable DNS service on this switch, first configure one or more name servers, and then enable domain lookup status.

To append domain names to incomplete host names received from a DNS client (For example, not formatted with dotted notation), you can specify a default domain name or a list of domain names to be tried in sequential order.

If there is no domain list, the default domain name is used. If there is a domain list, the default domain name is not used.

When an incomplete host name is received by the DNS server on this switch and a domain name list has been specified, the switch works through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.

When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Note: If all name servers are deleted, DNS is automatically disabled.

Command Attributes

Domain Lookup Status – Enables DNS host name-to-address translation.

Default Domain Name – Defines the default domain name appended to incomplete host names. Do not include the initial dot that separates the host name from the domain name. (Range: 1-64 alphanumeric characters)

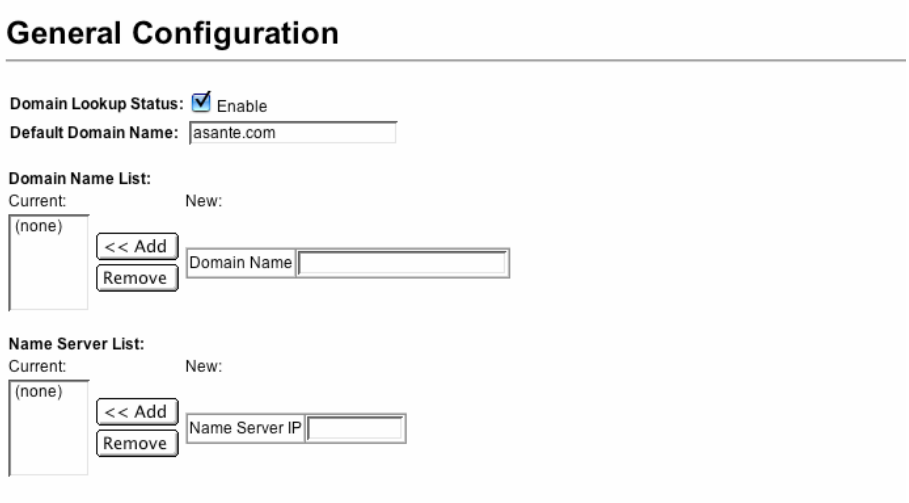
Domain Name List – Defines define a list of domain names that can be appended to incomplete host names. Do not include the initial dot that separates the host name from the domain name. (Range: 1-64 alphanumeric characters. 1-5 names)

Name Server List – Specifies the address of one or more domain name servers to use for name-to-address resolution. (Range: 1-6 IP addresses)

Configuring the Switch Using the Web or CLI

Web

Select DNS – General Configuration. Set the default domain name or list of domain names, specify one or more name servers to use to use for address resolution, enable domain lookup status, and click Apply.



CLI

This example sets a default domain name and a domain list. If a domain list is specified, the default domain name is not used.

```
Console(config)#ip domain-name sample.com
Console(config)#ip domain-list sample.com.uk
Console(config)#ip domain-list sample.com.jp
Console(config)#ip name-server 192.168.1.55 10.1.0.55
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.uk
    sample.com.jp
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

13.2 Static DNS Host to Address Entries

You can manually configure static entries in the DNS table that are used to map domain names to IP addresses.

13.2.1 Guidelines

Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.

Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name in the static table or via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

Field Attributes

Host Name – Name of a host device that is mapped to one or more IP addresses. (Range: 1-64 characters)

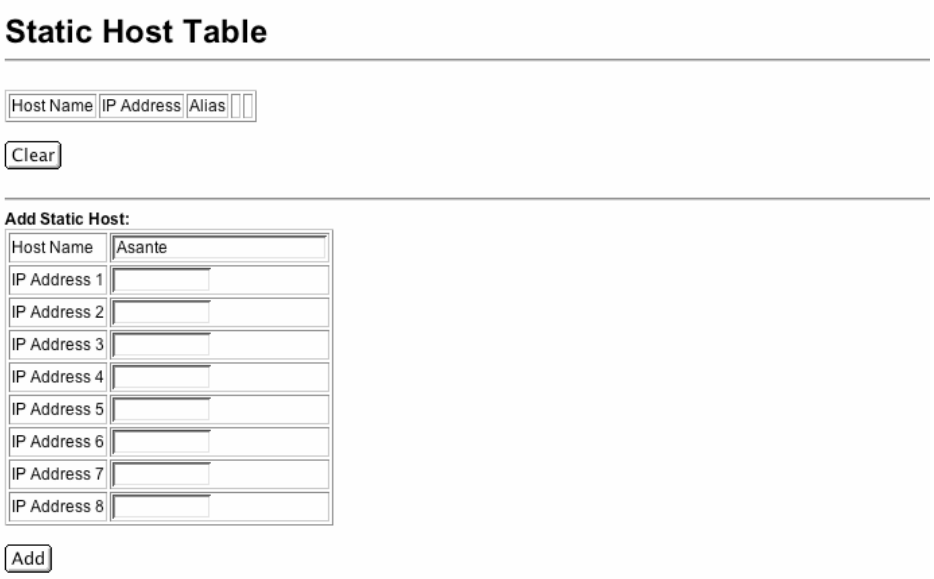
IP Address – Internet address(es) associated with a host name. (Range: 1-8 addresses)

Alias – Displays the host names that are mapped to the same address(es) as a previously configured entry.

Configuring the Switch Using the Web or CLI

Web

Select DNS – Static Host Table. Enter a host name and one or more corresponding addresses, then click Apply.



CLI

This example maps two address to a host name, and then configures an alias host name for the same addresses.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#ip host rd6 10.1.0.55
Console(config)#end
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
Console#
```

13.3 Displaying the DNS Cache

You can display entries in the DNS cache that have been learned via the designated name servers.

Field Attributes

No – The entry number for each resource record.

Flag – The flag is always “4” indicating a cache entry and therefore unreliable.

Type – This field includes CNAME, which specifies the canonical or primary name for the owner, and ALIAS, which specifies multiple domain names that are mapped to the same IP address as an existing entry.

IP – The IP address associated with this record.

TTL – The time to live reported by the name server.

Domain – The domain name associated with this record.

Configuring the Switch Using the Web or CLI

Web

Select DNS – Cache.

CLI

This example displays all the resource records learned from the designated name servers.

```
Console#show dns cache
NO       FLAG    TYPE    IP              TTL     DOMAIN
0         4      CNAME   207.46.134.222  51      www.microsoft.akadns.net
1         4      CNAME   207.46.134.190  51      www.microsoft.akadns.net
2         4      CNAME   207.46.134.155  51      www.microsoft.akadns.net
3         4      CNAME   207.46.249.222  51      www.microsoft.akadns.net
4         4      CNAME   207.46.249.27   51      www.microsoft.akadns.net
5         4      ALIAS   POINTER TO:4    51      www.microsoft.com
6         4      CNAME   207.46.68.27    71964   msn.com.tw
7         4      ALIAS   POINTER TO:6    71964   www.msn.com.tw
8         4      CNAME   65.54.131.192   605     passportimages.com
9         4      ALIAS   POINTER TO:8    605     www.passportimages.com
10        4      CNAME   165.193.72.190  87      global.msads.net
Console#
```

Chapter 14: Using the Command Line Interface

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "?" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Class	**Mode**
Exec	Normal
Privileged	Configuration
Global*	Access Control List
Interface	Line
Multiple Spanning Tree	VLAN Database

You must be in Privileged Exec mode to access the Global configuration mode. You must be in Global Configuration mode to access any of the other configuration modes.

14.1 Exec Commands

When you open a new console session on the switch with the user name and password "guest," the system enters the Normal Exec command mode (or guest mode), displaying the "Console>" command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password "admin." The system will now display the "Console#" command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the enable command, followed by the privileged level password "super"

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

      CLI session with the 44 10/100/1000 ports 4 Gigabit Combo ports
L2/L4 managed standalone switch is opened.
      To end the CLI session, enter [Exit].

Console#

Username: guest
Password: [guest login password]

      CLI session with the 44 10/100/1000 ports 4 Gigabit Combo ports
L2/L4 managed standalone switch is opened.
      To end the CLI session, enter [Exit].

Console#enable
Password: [privileged level password]
Console#
```

14.2 Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands only modify the running configuration. When the switch is rebooted, the start-up configuration is used. To store the running configuration use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

Global Configuration - These commands modify the system level configuration, and include commands such as hostname and snmp-server community.

Access Control List Configuration - These commands are used for packet filtering.

Interface Configuration - These commands modify the port configuration such as speed-duplex and negotiation.

Line Configuration - These commands modify the console port and Telnet configuration, and include command such as parity and databits.

VLAN Configuration - Includes the command to create VLAN groups.

Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.

To enter the Global Configuration mode, enter the command configure in Privileged Exec mode. The system prompt will change to “Console(config)#” which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the exit or end command to return to the Privileged Exec mode.

Mode	Command	Prompt
Line	line {console | vty}	Console(config-line)#
Interface	interface {ethernet port | port-channel id| vlan id}	Console(config-if)#
VLAN	vlan database	Console(config-vlan)#
MSTP	spanning-tree mst	Console(config-mstp)#

access-list ip standard	Console(config-std-acl)
access-list ip extended	Console(config-ext-acl)
access-list ip mask-precedence	Console(config-ip-mask-acl)
access-list mac	Console(config-mac-acl)

access-list mac mask-precedence	Console(config-mac-mask-acl)

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

14.3 Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group	Description
Line	Sets communication parameters for the serial port and Telnet, including baud rate and console time-out
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information
Flash/File	Manages code image or switch configuration files
Authentication	Configures logon access using local or remote authentication; also configures port security and IEEE 802.1x port access control
Access Control List	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)
SNMP	Activates authentication failure traps; configures community access strings, and trap managers; also configures IP address filtering
DHCP	Configures DHCP client
DNS	Configures DNS services.
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port
Rate Limiting	Controls the maximum rate for traffic transmitted or received on a port
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks
Address Table	Configures the address table for filtering specified addresses, displays current entries,

	clears the table, or sets the aging time
Spanning Tree	Configures Spanning Tree settings for the switch
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs and protocol VLANs
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for the bridge extension MIB
Priority	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for TCP traffic types, IP precedence, and DSCP
Multicast Filtering	Configures IGMP multicast filtering, query parameters, and specifies ports attached to a multicast router
IP Interface	Configures IP address for the switch

The access mode shown in the following tables is indicated by these abbreviations:

- ACL (Access Control List Configuration)
- GC (Global Configuration)
- IC (Interface Configuration)
- LC (Line Configuration)
- MST (Multiple Spanning Tree)
- NE (Normal Exec)
- PE (Privileged Exec)
- VC (VLAN Database Configuration)

Chapter 15: Configuration Guide

This chapter provides information about each of the features and an overview of the CLI commands needed to configure, manage and maintain the switch. For more complete information about the commands refer to **Chapter 16: Command Reference**.

15.1 Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (For example, a virtual terminal).

Command	Function	Mode
line	Identifies a specific line for configuration and starts the line configuration mode.	GC
login	Enables password checking at login.	LC
password	Specifies a password on a line.	LC
exec-timeout	Sets the interval that the command interpreter waits until input is detected.	LC
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts.	LC
silent-time	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command. This command only applies to the serial port.	LC
databits	Sets the number of data bits per character that are interpreted and generated by hardware. This command only applies to the serial port.	LC
parity	Defines the generation of a parity bit. This command only applies to the serial port.	LC
speed	Sets the terminal baud rate. This command only applies to the serial port.	LC
stopbits	Sets the number of the stop bits transmitted per byte. This command only applies to the serial port.	LC
disconnect	Terminates a line connection.	PE
show line	Displays a terminal line's parameters.	NE, PE

15.2 General Commands

The following table lists the general commands and describes the functions and command modes of each command.

Command	Function	Mode
enable	Activates privileged mode	NE

disable	Returns to normal mode from privileged mode	PE
configure	Activates global configuration mode	PE
show history	Shows the command history buffer	NE, PE
reload	Restarts the system	PE
end	Returns to Privileged Exec mode	any config. mode
exit	Returns to the previous configuration mode, or exits the CLI	any
quit	Exits a CLI session	NE, PE
help	Shows how to use help	any
?	Shows options for command completion (context sensitive)	any

15.2.1 Flash/File Commands

These commands are used to manage the system code or configuration files.

Command	Function	Mode
copy	Copies a code image or a switch configuration to or from flash memory or a TFTP server	PE
delete	Deletes a file or code image	PE
dir	Displays a list of files in flash memory	PE
whichboot	Displays the files booted	PE
boot system	Specifies the file or image used to start up the system	GC

15.3 System Management Commands

Use these commands to control system logs, passwords, user names, browser configuration options, and display or configure a variety of other system information.

The following table lists the system management commands and describes the functions of each command.

Command Group	Function
Device Designation	Configures information that uniquely identifies this switch
User Access	Configures the basic user names and passwords for management access
IP Filter	Configures IP addresses that are allowed management access
Web Server	Enables management access via a Web browser

Secure Shell	Provides secure replacement for Telnet
Event Logging	Controls logging of error messages
SMTP Alerts	Configures SMTP email alerts
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually
System Status	Displays system configuration, active managers, and version information
Frame Size	Enables support for jumbo frames

15.3.1 Device Designation Commands

The following table lists the device designation commands and describes the functions and command modes of each command.

Command	Function	Mode
Prompt	Customizes the prompt used in PE and NE mode	GC
hostname	Specifies the host name for the switch	GC
snmp-server contact	Sets the system contact string	GC
snmp-server location	Sets the system location string	GC

15.3.2 User Access Commands

The basic commands required for management access are listed in this section. This switch also includes other options for password checking through the console or a Telnet connection, user authentication through a remote authentication server and host access authentication for specific ports.

The following table lists the user access commands and describes the functions and command modes of each command.

Command	Function	Mode
Username	Establishes a user name-based authentication system at login	GC
Enable password	Sets a password to control access to the Privileged Exec level	GC

15.3.3 IP Filter Commands

The following table lists the filter commands and describes the functions and command modes of each command.

Command	Function	Mode
management	Configures IP addresses that are allowed management access	GC
show management	Displays the switch to be monitored or configured from a browser	PE

15.3.4 Web Server Commands

The following table lists the web server commands and describes the functions and command modes of each command.

Command	Function	Mode
ip http port	Specifies the port to be used by the Web browser interface	GC
ip http server	Allows the switch to be monitored or configured from a browser	GC
ip http secure-server	Enables HTTPS/SSL for encrypted communications	GC
ip http secure-port	Specifies the UDP port number for HTTPS/SSL	GC

15.3.5 Secure Shell Commands

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as rlogin (remote login), rsh (remote shell), and rcp (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When a client contacts the switch via the SSH protocol, the switch uses a public-key that the client must match along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

This section describes the commands used to configure the SSH server. You also need to install a SSH client on the management station when using this protocol to configure the switch.

Note: The switch supports both SSH Version 1.5 and 2.0.

The following table lists the filter commands and describes the functions and command modes of each command.

Command	Function	Mode
ip ssh server	Enables the SSH server on the switch	GC
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC
ip ssh server-key size	Sets the SSH server key size	GC
copy tftp public-key	Copies the user's public key from a TFTP server to the switch	PE
delete public-key	Deletes the public key for the specified user	PE
ip ssh crypto host-key generate	Generates the host key	PE

ip ssh crypto zeroize	Clear the host key from RAM	PE
ip ssh save host-key	Saves the host key from RAM to flash memory	PE
disconnect	Terminates a line connection	PE
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE
show ssh	Displays the status of current SSH sessions	PE
show public-key	Shows the public key for the specified user or for the host	PE
show users	Shows SSH users, including privilege level and public key type	PE

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the **authentication login** command. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the ip ssh crypto host-key generate command to create a host public/private key pair.

2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

```
10.1.0.54 1024 35 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761177
```

3. Import Client's Public Key to the Switch – Use the copy tftp public-key command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch using the User Accounts page as described in section **6.1.1 Configuring User Accounts**.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA Version 1 key:

```
1024 35 134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19
```

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. Enable SSH Service – Use the ip ssh server command to enable the SSH server on the switch.

6. Configure Challenge-Response Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only

clients that have a private key corresponding to the public keys stored on the switch can gain access. The following exchanges take place during this process:

- The client sends its public key to the switch.
- The switch compares the client's public key to those stored in memory.
- If a match is found, the switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.
- The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.
- The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. You do not need to configure the client's keys.

15.3.6 Event Logging Commands

The following table lists the even logging commands.

Command	Function	Mode
logging on	Controls logging of error messages	GC
logging history	Limits syslog messages saved to switch memory based on severity	GC
logging host	Adds a syslog server host IP address that will receive logging messages	GC
logging facility	Sets the facility type for remote logging of syslog messages	GC
logging trap	Limits syslog messages saved to a remote server based on severity	GC
clear logging	Clears messages from the logging buffer	PE
show logging	Displays the state of logging configuration	PE

15.3.7 SMTP Alert Commands

Configures SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Command	Function	Mode
logging sendmail host	SMTP servers to receive alert messages	GC
logging sendmail level	Severity threshold used to trigger alert messages	GC
logging sendmail source-email	Email address used for "From" field of alert messages	GC

logging sendmail destination-email	Email recipients of alert messages	GC
logging sendmail	Enables SMTP event handling	GC
show logging sendmail	Displays SMTP event handler settings	NE, PE

15.3.8 Time Commands

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP), or by using information broadcast by local time servers.

Command	Function	Mode
sntp client	Accepts time from specified time servers	GC
sntp server	Specifies one or more time servers	GC
sntp poll	Sets the interval at which the client polls for time	GC
sntp broadcast client	Accepts time from any time broadcast server	GC
show sntp	Shows current SNTP configuration settings	NE, PE
clock timezone	Sets the time zone for the switch's internal clock	GC
Calendar set	Sets the system date and time	PE
show calendar	Displays the current date and time setting	NE, PE

15.3 9 System Status Commands

The following table lists the system status commands.

Command	Function	Mode
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE
show running-config	Displays the configuration data currently in use	PE
show system	Displays system information	NE, PE
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE
show version	Displays version information for the system	NE, PE

15.3.10 Frame Size Commands

The following table lists the frame size commands.

Command	Function	Mode

jumbo frame	Enables support for jumbo frames	GC

15.4 Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or RADIUS authentication methods. You can also enable port-based authentication for network client access using IEEE 802.1x.

The following table lists the authentication commands and describes the functions and command modes of each command.

Command Mode	Function
Authentication Sequence	Defines logon authentication method and precedence
RADIUS Client	Configures settings for authentication via a RADIUS server
TACACS+ Client	Configures settings for authentication via a TACACS+ server
Port Security	Configures secure addresses for a port
Port Authentication	Configures host authentication on specific ports using 802.1x

15.4.1 Authentication Sequence

The following table lists the authentication sequence commands.

Command	Function	Mode
authentication login	Defines logon authentication method and precedence	GC
authentication enable	Defines the authentication method and precedence for command mode change	GC

15.4.2 RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Command	Function	Mode
radius-server host	Specifies the RADIUS server	GC
radius-server port	Sets the RADIUS server network port	GC
radius-server key	Sets the RADIUS encryption key	GC
radius-server retransmit	Sets the number of retries	GC
radius-server timeout	Sets the interval between sending authentication requests	GC

show radius-server	Shows the current RADIUS settings	PE

15.4.3 TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Command	Function	Mode
tacacs-server host	Specifies the TACACS+ server	GC
tacacs-server port	Specifies the TACACS+ server network port	GC
tacacs-server key	Sets the TACACS+ encryption key	GC
show tacacs-server	Shows the current TACACS+ settings	GC

15.4.4 Port Security Commands

These commands can be used to disable the learning function or manually specify secure addresses for a port. You can leave port security off for an initial training period (for example, enable the learning function) to register all the current VLAN members on the selected port, and then enable port security. Doing this helps that the port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port.

Command	Function	Mode
port security	Configures a secure port	IC
mac-address-table static	Maps a static address to a port in a VLAN	GC
show mac-address-table	Displays entries in the bridge-forwarding database	PE

15.4.5 The 802.1x Port Authentication

The switch supports IEEE 802.1x (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Command	Function	Mode
authentication dot1x default	Sets the default authentication server type	GC
dot1x default	Resets all dot1x parameters to their default values	GC
dot1x max-req	Sets the maximum number of times the switch retransmits an EAP request/identity packet to the client before it times	GC
dot1x port-control	Sets dot1x mode for a port interface	IC

dot1x operation-mode	Allows single or multiple hosts on an dot1x port	IC
dot1x re-authenticate	Forces re-authentication on specific ports	PE
dot1x re-authentication	Enables re-authentication for all ports	GC
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	GC
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	GC
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	GC
show dot1x	Shows all dot1x related information	PE

15.5 Access Control List Commands

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

There are three filtering modes:

- Standard IP ACL mode (STD-ACL) filters packets based on the source IP address.
- Extended IP ACL mode (EXT-ACL) filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the TCP protocol is specified, then you can also filter packets based on the TCP control code.
- MAC ACL mode (MAC-ACL) filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

The following restrictions apply to ACLs:

- This switch supports ACLs for both ingress and egress filtering. You can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- The average number of rules bound the ports should not exceed 20.

- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- The switch does not support the explicit “deny any any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.
- Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Egress MAC ACL for egress ports.
2. User-defined rules in the Egress IP ACL for egress ports.
3. User-defined rules in the Ingress MAC ACL for ingress ports.
4. User-defined rules in the Ingress IP ACL for ingress ports.
5. Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
6. Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.
7. If no explicit rule is matched, the implicit default is permit all.

Masks for Access Control Lists

You can specify optional masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny the rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ACL. A mask must be bound exclusively to one of the basic ACL types (For example, Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Command Groups	Function
IP ACLs	Configures ACLs based on IP addresses, TCP/UDP port number, protocol type, and TCP control code
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port

15.5.1 IP ACLs

The following table lists the IP access control list commands.

Command	Function	Mode
access-list ip	Creates an IP ACL and enters configuration mode	GC
permit, deny	Filters packets matching a specified source IP address	STD-ACL

permit, deny	Filters packets meeting the specified criteria, including source and destination IP address, TCP/UDP port number, protocol type, and TCP control code	EXT-ACL
show ip access-list	Displays the rules for configured IP ACLs	PE
access-list ip mask-precedence	Changes to the mode for configuring access control masks	GC
Mask	Sets a precedence mask for the ACL rules	IP-Mask
show access-list ip mask-precedence	Shows the ingress or egress rule masks for IP ACLs	PE
ip access-group	Adds a port to an IP ACL	IC
show ip access-group	Shows port assignments for IP ACLs	PE
map access-list ip	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC
show map access-list ip	Shows CoS value mapped to an access list for an interface	PE
match access-list ip	Changes the 802.1p priority, IP Precedence, or DSCP Priority of a frame matching the defined rule (For example, also called packet marking)	IC
show marking	Displays the current configuration for packet marking	PE

15.5.2 MAC ACLs

The following table lists the MAC access control list commands.

Command	**Function**	**Mode**
access-list mac	Creates a MAC ACL and enters configuration mode	GC
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL
show mac access-list	Displays the rules for configured MAC ACLs	PE
access-list mac mask-precedence	Changes to the mode for configuring access control masks	GC
Mask	Sets a precedence mask for the ACL rules	MAC-Mask
show access-list mac mask-precedence	Shows the ingress or egress rule masks for MAC ACLs	PE
mac access-group	Adds a port to a MAC ACL	IC
show mac access-group	Shows port assignments for MAC ACLs	PE

map access-list mac	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC
show map access-list mac	Shows CoS value mapped to an access list for an interface	PE
match access-list mac	Changes the 802.1p priority the priority of a frame matching the defined rule (For example, also called packet marking)	IC
show marking	Displays the current configuration for packet marking	PE

15.5.3 ACL Information

The following table lists the commands used to show information about ACLs.

Command	Function	Mode
show access-list	Show all ACLs and associated rules	PE
show access-group	Shows the ACLs assigned to each port	PE

15.6 SNMP Commands

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

Command	Function	Mode
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC
snmp-server contact	Sets the system contact string	GC
snmp-server location	Sets the system location string	GC
snmp-server host	Specifies the recipient of an SNMP notification operation	GC
snmp-server enable traps	Enables the device to send SNMP traps (For example, SNMP notifications)	GC
show snmp	Displays the status of SNMP communications	NE, PE

15.7 DHCP Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client. You can configure any VLAN interface to be automatically assigned an IP address via DHCP.

DHCP Client

Command	Function	Mode
ip dhcp restart	Submits a BOOTP or DHCP client request	PE

15.7.1 DNS Commands

These commands are used to configure Domain Naming System (DNS) services. You can manually configure entries in the DNS domain name to IP address mapping table, configure default domain names, or specify one or more name servers to use for domain name to address translation.

Domain name services is not be enabled until at least one name server is specified with the ip name-server command and domain lookup is enabled with the ip domain-lookup command.

Command	Function	Mode
ip host	Creates a static host name-to-address mapping	GC
clear host	Deletes entries from the host name-to-address table	PE
ip domain-name	Defines a default domain name for incomplete host names	GC
ip domain-list	Defines a list of default domain names for incomplete host names	GC
ip name-server	Specifies the address of one or more name servers to use for host name-to-address translation	GC
ip domain-lookup	Enables DNS-based host name-to-address translation	GC
show hosts	Displays the static host name-to-address mapping table	PE
show dns	Displays the configuration for DNS services	PE
show dns cache	Displays entries in the DNS cache	PE
clear dns cache	Clears all entries from the DNS cache	PE

15.8 Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Command	Function	Mode
Interface	Configures an interface type and enters interface configuration mode	GC
description	Adds a description to an interface configuration	IC
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC
negotiation	Enables autonegotiation of a given interface	IC
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC
flowcontrol	Enables flow control on a given interface	IC
combo-forced-mode	Force port type selected for combination ports	IC

shutdown	Disables an interface	IC
switchport broadcast packet-rate	Configures the broadcast storm control threshold	IC
clear counters	Clears statistics on an interface	PE
show interfaces status	Displays status for the specified interface	NE, PE
show interfaces counters	Displays statistics for the specified interfaces	NE, PE
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE

15.9 Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

Command	Function	Mode
port monitor	Configures a mirror session	IC
show port monitor	Shows the configuration for a mirror port	PE

15.10 Rate Limit Commands

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command	Function	Mode
rate-limit	Configures the maximum input or output rate for a port	IC

15.11 Link Aggregation Commands

Ports can be statically grouped into an aggregate link (For example, trunk) to increase the bandwidth of a network connection or to ensure fault recovery. You can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

The following table lists the manual configuration commands.

Command	Function	Mode
interface port-channel	Enters interface configuration mode and Configures a trunk	GC
Channel-group	Adds a port to a trunk	IC (Ethernet)
Dynamic Configuration Command		
lacp	Configures LACP for the current interface	IC (Ethernet)
lacp system-priority	Configures a port's LACP system priority	IC (Ethernet)
lacp admin-key	Configures a port's administration key	IC (Ethernet)
lacp admin-key	Configures an port channel's administration key	IC (Port Channel)
lacp port-priority	Configures a port's LACP port priority	IC (Ethernet)
Trunk Status Display Command		
show interfaces status port-channel	Shows trunk information	NE, PE
show lacp	Shows LACP information	PE

Guidelines for Creating Trunks

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to eight ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including communication mode (For example, speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

Dynamically Creating a Port Channel

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (For example, it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.

- If the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

15.12 Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Command	Function	Mode
mac-address-table static	Maps a static address to a port in a VLAN	GC
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE
show mac-address-table	Displays entries in the bridge-forwarding database	PE
mac-address-table aging-time	Sets the aging time of the address table	GC
show mac-address-table aging-time	Shows the aging time for the address table	PE

15.13 Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Command	Function	Mode
spanning-tree	Enables the spanning tree protocol	GC
spanning-tree mode	Configures STP, RSTP or MSTP mode	GC
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC
spanning-tree priority	Configures the spanning tree bridge priority	GC
spanning-tree path-cost method	Configures the path cost method for RSTP/MSTP	GC
spanning-tree transmission-limit	Configures the transmission limit for RSTP/MSTP	GC
spanning-tree mst-configuration	Changes to MSTP configuration mode	GC

mst vlan	Adds VLANs to a spanning tree instance	MST
mst priority	Configures the priority of a spanning tree instance	MST
Name	Configures the name for the multiple spanning tree	MST
Revision	Configures the revision number for the multiple spanning tree	MST
max-hops	Configures the maximum number of hops allowed in the region before a BPDU is discarded	MST
spanning-tree spanning-disabled	Disables spanning tree for an interface	IC
spanning-tree cost	Configures the spanning tree path cost of an interface	IC
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC
spanning-tree edge-port	Enables fast forwarding for edge ports	IC
spanning-tree portfast	Sets an interface to fast forwarding	IC
spanning-tree link-type	Configures the link type for RSTP/MSTP	IC
spanning-tree mst cost	Configures the path cost of an instance in the MST	IC
spanning-tree mst port-priority	Configures the priority of an instance in the MST	IC
show spanning-tree	Shows spanning tree configuration for the common spanning tree (For example, overall bridge), a selected interface, or an instance within the multiple spanning tree	PE
show spanning-tree mst configuration	Shows the multiple spanning tree configuration	PE

15.14 VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Command Groups	**Function**
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports

Configuring Protocol VLANs	Configures protocol-based VLANs based on frame type and protocol

15.14.1 Editing VLANs

The following table list the commands for editing VLAN groups.

Command	Function	Mode
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC
vlan	Configures a VLAN, including VID, name and state	VC

15.14.2 Configuring VLAN Interfaces

Command	Function	Mode
Interface vlan	Enters interface configuration mode for a specified VLAN	IC
switchport mode	Configures VLAN membership mode for an interface	IC
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC
switchport ingress-filtering	Enables ingress filtering on an interface	IC
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC
switchport allowed vlan	Configures the VLANs associated with an interface	IC
switchport gvrp	Enables GVRP for an interface	IC
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC

15.14.3 Displaying VLAN Information

The following table lists the commands need to show VLAN information.

Command	Function	Mode
show vlan	Shows VLAN information	NE, PE
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE

15.14.4 Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This section describes commands used to configure private VLANs.

Command	Function	Mode
Pvlan	Enables and configured private VLANS	GC
show pvlan	Displays the configured private VLANS	PE

15.14.5 Configuring Protocol-based VLANs Using the CLI

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

Command	Function	Mode
Protocol-vlan protocol-group	Create a protocol group, specifying the supported protocols	GC
Protocol-vlan protocol-group	Maps a protocol group to a VLAN	IC
show protocol-vlan protocol-group	Shows the configuration of protocol groups	PE
show interfaces protocol-vlan protocol-group	Shows the interfaces mapped to a protocol group and the corresponding VLAN	PE

To configure protocol-based VLANs, follow these steps:

1. Configure VLAN groups for the protocols you want to use (see **15.14.2**). Although not mandatory, you should suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.

2. Create a protocol group for each of the protocols you want to assign to a VLAN using the protocol-vlan protocol-group command (General Configuration mode).

3. Then map the protocol for each interface to the appropriate VLAN using the protocol-vlan protocol-group command (Interface Configuration mode).

15.15 GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Command	Function	Mode
bridge-ext gvrp	Enables GVRP globally for the switch	GC

show bridge-ext	Shows the global bridge extension configuration	PE
switchport gvrp	Enables GVRP for an interface	IC
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC
show gvrp configuration	Displays GVRP configuration for the selected interface	NE, PE
garp timer	Sets the GARP timer for the selected function	IC
show garp timer	Shows the GARP timer for the selected function	NE, PE

15.16 Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Command Groups	Function
Priority (Layer 2)	Configures default priority for untagged frames, sets queue weights, and maps class of service tags to hardware queues
Priority (Layer 3 and 4)	Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values

15.16.1 Priority Commands (Layer 2)

The following table lists the layer 2 priority commands.

Command	Function	Mode
switchport priority default	Sets a port priority for incoming untagged frames	IC
queue mode	Sets the queue mode to strict priority or Weighted Round-Robin (WRR)	GC
queue bandwidth	Assigns round-robin weights to the priority queues	GC
queue cos map	Assigns class-of-service values to the priority queues	IC
show queue mode	Shows the current queue mode	PE
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE
show queue cos-map	Shows the class-of-service map	PE
show interfaces switchport	Displays the administrative and operational status of an interface	PE

15.16.2 Priority Commands (Layer 3 and 4)

The following table lists the layer 3 and 4 priority commands.

Command	Function	Mode
map ip port	Enables TCP class of service mapping	GC
map ip port	Maps TCP socket to a class of service	IC
map ip precedence	Enables IP precedence class of service mapping	GC
map ip precedence	Maps IP precedence value to a class of service	IC
map ip dscp	Enables IP DSCP class of service mapping	GC
map ip dscp	Maps IP DSCP value to a class of service	IC
map access-list ip	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC
map access-list mac	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC
show map access-list ip	Shows CoS value mapped to an access list for an interface	PE
show map access-list mac	Shows CoS value mapped to an access for an interface	PE
show map ip port	Shows the IP port map	PE
show map ip precedence	Shows the IP precedence map	PE
show map ip dscp	Shows the IP DSCP map	PE

15.17 Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it continues to receive the multicast service.

Command Groups	Function
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, displays current snooping and query settings, and displays the multicast service and group members
IGMP Query	Configures IGMP query parameters for multicast filtering at Layer 2
Static Multicast Routing	Configures static multicast router ports

15.17.1 IGMP Snooping Commands

The following table lists the IGMP snooping commands.

Command	Function	Mode
ip igmp snooping	Enables IGMP snooping	GC
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC
ip igmp snooping version	Configures the IGMP version for snooping	GC
show ip igmp snooping	Shows the IGMP snooping and query configuration	PE
show mac-address-table multicast	Shows the IGMP snooping MAC multicast list	PE

15.17.2 IGMP Query Commands (Layer 2)

The following table lists the IGMP layer 2 query commands.

Command	Function	Mode
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC
ip igmp snooping query-count	Configures the query count	GC
ip igmp snooping query-interval	Configures the query interval	GC
ip igmp snooping query-max-response-time	Configures the report delay	GC
ip igmp snooping router-port-expire-time	Configures the query timeout	GC

15.17.3 Static Multicast Routing Commands

The following table lists the static multicast routing commands.

Command	Function	Mode
ip igmp snooping vlan mrouter	Adds a multicast router port	GC
show ip igmp snooping mrouter	Shows multicast router ports	PE

15.18 IP Interface Commands

There are no IP addresses assigned to this switch by default. You must manually configure a new address to manage the switch over your network. You may also need to a establish a default gateway between this device and management stations or other devices that exist on another network segment.

The following table lists the basic IP configuration commands.

Command	Function	Mode
ip address	Sets the IP address for the current interface	IC
ip default-gateway	Defines the default gateway through which this switch can reach other subnetworks	GC
show ip interface	Displays the IP settings for this device	PE
show ip redirects	Displays the default gateway configured for this device	PE
ping	Sends ICMP echo request packets to another node on the network	NE, PE

Chapter 16: Command Reference

The section contains an alphabetical listing of all the commands used to configure, manage and maintain your switch. Refer to **Chapter 15: Configuration Guide,** for information on specific features and associated commands.

16.1 access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IP ACLs. Use the no form to remove the specified ACL.

Syntax Description

```
[no] access-list ip {standard | extended} acl_name
```

Standard	Specifies an ACL that filters packets based on the source IP address.
Extended	Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
acl_name	Name of the ACL. (Maximum length: 16 characters)

Default

None

Command Mode

Global Configuration

Usage Guidelines

An egress ACL must contain all deny rules.

When you create a new ACL or enter configuration mode for an existing ACL, use the permit or deny command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.

To remove a rule, use the no permit or no deny command followed by the exact text of a previously configured rule.

An ACL can contain up to 32 rules.

Example

The following is sample output from the access-list command with the ip argument.

```
Console(config)#access-list ip standard james
Console(config-std-acl)#
```

Related Commands

permit, deny

ip access-group

show ip access-list

16.2 access-list ip mask-precedence

This command changes to the IP Mask mode used to configure access control masks. Use the no form to delete the mask table.

Syntax Description

```
[no] access-list ip mask-precedence {in | out}
```

In	Ingress mask for ingress ACLs.
Out	Egress mask for egress ACLs.

Default

Default system mask: Filter inbound packets according to specified IP ACLs.

Command Mode

Global Configuration

Usage Guidelines

A mask can only be used by all ingress ACLs or all egress ACLs.

The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; For example, the first mask that matches a rule will determine the rule that is applied to a packet.

You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

Example

The following is sample output from the access-list command with the ip mask-precedence argument.

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#
```

Related Commands

mask (IP ACL)

ip access-group

16.3 access-list mac

This command adds a MAC access list and enters MAC ACL configuration mode. Use the no form to remove the specified ACL.

Syntax Description

[**no**] access-list mac *acl_name*

acl_name	Name of the ACL. (Maximum length: 16 characters)

Default

None

Command Mode

Global Configuration

Usage Guidelines

An egress ACL must contain all deny rules.

When you create a new ACL or enter configuration mode for an existing ACL, use the permit or deny command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.

To remove a rule, use the no permit or no deny command followed by the exact text of a previously configured rule.

An ACL can contain up to 32 rules.

Example

The following is sample output from the access-list command with the mac argument.

```
Console(config)#access-list mac james
Console(config-mac-acl)#
```

Related Commands

permit, deny

mac access-group

show mac access-list

16.4 access-list mac mask-precedence

This command changes to MAC Mask mode used to configure access control masks. Use the no form to delete the mask table.

Syntax Description

[**no**] access-list ip mask-precedence {in | out}

In	Ingress mask for ingress ACLs.
Out	Egress mask for egress ACLs.

Default

Default system mask: Filter inbound packets according to specified MAC ACLs.

Command Mode

Global Configuration

Usage Guidelines

You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

A mask can only be used by all ingress ACLs or all egress ACLs.

The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; For example, the first mask that matches a rule will determine the rule that is applied to a packet.

Example

The following is sample output from the access-list command with the mac mask-precedence argument.

```
Console(config)#access-list mac  mask-precedence in
Console(config-mac-mask-acl)#
```

Related Commands

mask (MAC ACL)

mac access-group

16.5 authentication dot1x default

This command sets the default authentication server type. Use the no form to restore the default.

Syntax Description

```
authentication dot1x default radius
```

```
no authentication dot1x
```

Default

RADIUS

Command Mode

Global Configuration

Example

The following is sample output from the authentication command with the dot1x argument.

```
Console(config)#authentication dot1x default radius
```

```
Console(config)#
```

16.6 authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the **enable** command in Chpater 16. Use the no form to restore the default.

Syntax Description

```
authentication enable {[local] [radius] [tacacs]}

no authentication enable
```

Local	Use local password only.
radius	Use RADIUS server password only.
tacacs	Use TACACS server password.

Default

Local

Command Mode

Global Configuration

Usage Guidelines

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.

You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter “authentication enable radius tacacs local,” the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

The following is sample output from the authentication enable command.

```
Console(config)#authentication enable radius
Console(config)#
```

Related Commands

enable password

16.7 authentication login

This command defines the login authentication method and precedence. Use the no form to restore the default.

Syntax Description

```
authentication login {[local] [radius] [tacacs]}

no authentication login
```

Local	Use local password.
radius	Use RADIUS server password.
tacacs	Use TACACS server password.

Default

Local

Command Mode

Global Configuration

Usage Guidelines

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.

You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter “authentication login radius tacacs local,” the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

The following is sample output from the authentication login command.

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

username

16.8 boot system

This command specifies the image used to start up the system.

Syntax Description

`boot system {boot-rom| config | opcode}: filename`

The type of file or image to set as a default includes:

boot-rom	Boot ROM.
Config	Configuration file.
opcode	Run-time operation code.
filename	Name of the configuration file or image name. The colon (:) is required before the filename.

Default

None

Command Mode

Global Configuration

Usage Guidelines

A colon (:) is required after the specified file type.

If the file contains an error, it cannot be set as the default file.

Example

The following is sample output from the boot command with the system argument.

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir

whichboot

16.9 bridge-ext gvrp

This command enables GVRP globally for the switch. Use the no form to disable it.

Syntax Description

`[no] bridge-ext gvrp`

Default

Disabled

Command Mode

Global Configuration

Usage Guidelines

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs that extend beyond the local switch.

Example

The following is sample output from the bridge-ext gvrp command.

```
Console(config)#bridge-ext gvrp
Console(config)#
```

16.10 calendar set

This command sets the system clock.

Syntax Description

`calendar set` *`hour min sec`* {*`day month year`* | *`month day year`*}

Hour	Hour in 24-hour format. (Range: 0 - 23)
Min	Minute. (Range: 0 - 59)
Sec	Second. (Range: 0 - 59)
Day	Day of month. (Range: 1 – 31)
month	january | february | march | april | may | june | july | august | september | october | november | december
Year	Year (4-digit). (Range: 2001 - 2101)

Default

None

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, August 1st, 2004.

```
Console#calendar set 15 12 34 1 August 2004
Console#
```

16.11 capabilities

This command advertises the port capabilities of a given interface during autonegotiation. Use the no form with parameters to remove an advertised capability, or the no form without parameters to restore the default values.

Syntax Description

```
[no] capabilities {1000full | 100full | 100half | 10full | 10half |
flowcontrol | symmetric}
```

1000full	Supports 1000 Mbps full-duplex operation
100full	Supports 100 Mbps full-duplex operation
100half	Supports 100 Mbps half-duplex operation
10full	Supports 10 Mbps full-duplex operation
10half	Supports 10 Mbps half-duplex operation
flowcontrol	Supports flow control
symmetric (Gigabit only)	When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (The current switch ASIC only supports symmetric pause frames.)

Default

100BASE-TX: 10half, 10full, 100half, 100full

1000BASE-T: 10half, 10full, 100half, 100full, 1000full

1000BASE-SX/LX/LH: 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

When auto-negotiation is enabled with the negotiation command, the switch will negotiate the best settings for a link based on the capabilities command. When auto-negotiation is disabled, you must manually specify the link attributes with the speed-duplex and flowcontrol commands.

Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

negotiation

speed-duplex

flowcontrol

16.12 channel-group

This command adds a port to a trunk. Use the no form to remove a port from a trunk.

Syntax Description

`channel-group` *`channel-id`*

`no` `channel-group`

channel-id	Trunk index (Range: 1-6)

Default

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.

Use no channel-group to remove a port group from a trunk.

Use no interfaces port-channel to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

16.13 clear counters

This command clears statistics on an interface.

Syntax Description

`clear counters` *`interface`*

Interface	ethernet unit/port unit – This is device 1. port - Port number.
Port-channel	Channel-id (Range: 1-6)

Default

None

Command Mode

Privileged Exec

Usage Guidelines

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. If you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

16.14 clear dns cache

This command clears all entries in the DNS cache.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the clear dns cache command the viewing the results using the show dns cache command/

```
Console#clear dns cache
Console#show dns cache
NO      FLAG    TYPE    IP              TTL     DOMAIN
Console#
```

Related Commands

show dns cache

16.15 clear host

This command deletes entries from the DNS table.

Syntax Description

```
clear host {name | *}
```

Name	Name of the host. (Range: 1-64 characters)
*	Removes all entries.

Default

None

Command Mode

Privileged Exec

Example

This example clears all static entries from the DNS table.

```
Console#clear host *
Console#
```

16.16 clear logging

This command clears messages from the log buffer.

Syntax Description

```
clear logging [flash | ram]
```

flash	Event history stored in flash memory (For example, permanent memory).
ram	Event history stored in temporary RAM (For example, memory flushed on power reset).

Default

Flash and RAM

Command Mode

Privileged Exec

Example

The following example shows using the clear logging command.

```
Console#clear logging
Console#
```

Related Commands

show logging

16.17 clear mac-address-table dynamic

This command removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the clear command using the mac-address argument.

```
Console#clear mac-address-table dynamic
```

16.18 clock timezone

This command sets the time zone for the switch's internal clock.

Syntax Description

clock timezone *name* hour *hours* minute *minutes* {before-utc | after-utc}

Name	Name of timezone, usually an acronym. (Range: 1-29 characters)
Hours	Number of hours before/after UTC. (Range: 0-12 hours)
Minutes	Number of minutes before/after UTC. (Range: 0-59 minutes)
before-utc	Sets the local time zone before (east) of UTC.
after-utc	Sets the local time zone after (west) of UTC.

Default

None

Command Mode

Global Configuration

Usage Guidelines

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

The following is an example of using the clock timezone command.

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

show sntp

16.19 combo-forced-mode

This command forces the port type selected for combination ports 21-24/45-48. Use the no form to restore the default mode.

Syntax Description

`combo-forced-mode` *mode*

no `combo-forced-mode`

Mode	**copper-forced** - Always uses the built-in RJ-45 port. **copper-preferred-auto** - Uses the built-in RJ-45 port if both combination types are functioning and the RJ-45 port has a valid link. **sfp-forced** - Always uses the SFP port (even if module not installed). **sfp-preferred-auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

Default

sfp-preferred-auto

Command Mode

Interface Configuration (Ethernet)

Example

The following example shows forcing the switch to use the built-in RJ-45 port for the combination port 48.

```
Console(config)#interface ethernet 1/48
Console(config-if)#combo-forced-mode copper-forced
Console(config-if)#
```

16.20 configure

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration. See section **14.5 Understanding Command Modes**.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output using the configure command.

```
Console#configure
Console(config)#
```

Related Commands

end

16.21 copy

This command moves (upload/download) a code image or configuration file between the switch's flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax Description

```
copy file {file | running-config | startup-config | tftp}

copy running-config {file | startup-config | tftp}

copy startup-config {file | running-config | tftp}

copy tftp {file | running-config | startup-config | https-certificate |
public-key}
```

file	Keyword that allows you to copy to/from a file.
running-config	Keyword that allows you to copy to/from the current running configuration.
Startup-config	The configuration used for system initialization.
tftp	Keyword that allows you to copy to/from a TFTP server.
https-certificate	Copies an HTTPS certificate from an TFTP server to the switch.

public-key	Keyword that allows you to copy a SSH key from a TFTP server.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

The system prompts for data required to complete the copy command.

The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Due to the size limit of the flash memory, the switch supports only two operation code files.

The maximum number of user-defined configuration files depends on available memory.

You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.

To replace the startup configuration, you must use startup-config as the destination.

The Boot ROM and Loader cannot be uploaded or downloaded from the TFTP server. You must use a direct console connection and access the download menu during a boot up to download the Boot ROM (or diagnostic) image. See **Appendix B: Upgrading Firmware via the Serial Port** for more informaiton.

For information on specifying an https-certificate, see section **6.3.2 Replacing the Default Secure-site Certificate**. For information on configuring the switch to use HTTPS/SSL for a secure connection, see **ip http secure-server** command.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
```

```
\Write to FLASH finish.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

The following example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

The following example shows coping a public-key used by SSH from an TFTP server. Note that public key authentication via SSH is only supported for users configured locally on the switch:

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1. RSA:  2. DSA: <1-2>: 1
Source file name: asante_start
Username: asante
TFTP Download
Success.
Write to FLASH Programming.
Success.



Console#
```

16.22 databits

This command sets the number of data bits per character that are interpreted and generated by the console port. Use the no form to restore the default value.

Syntax Description

```
databits {7 | 8}

no databits
```

7	Seven data bits per character.
8	Eight data bits per character.

Default

8 data bits per character

Command Mode

Line Configuration

Usage Guidelines

The databits command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity

16.23 delete

This command deletes a file or image.

Syntax Description

```
delete filename
```

filename	Name of the configuration file or image name.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

If the file type is used for system startup, then this file cannot be deleted.

“Factory_Default_Config.cfg” cannot be deleted.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir

delete public-key

16.24 delete public-key

Use this command to delete the specified user’s public key.

Syntax Description

`delete public-key` *`username`* `[dsa | rsa]`

username	Name of an SSH user. (Range: 1-8 characters)
Dsa	DSA public key type.
Rsa	RSA public key type.

Default

Deletes both the DSA and RSA key.

Command Mode

Privileged Exec

Example

The following example shows using the public-key command with the dsa argument.

```
Console#delete public-key admin dsa
Console#
```

16.25 description

This command adds a description to an interface. Use the no form to remove the description.

Syntax Description

`description` *`string`*

`no` `description`

String	Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to port 24.

```
Console(config)#interface ethernet 1/24
Console(config-if)#description RD-SW#3
Console(config-if)#
```

16.26 dir

This command displays a list of files in flash memory.

Syntax Description

`dir [boot-rom | config | opcode [:`*`filename`*`]]`

The type of file or image to display includes:

boot-rom	Boot ROM (or diagnostic) image file.
Config	Switch configuration file.
opcode	Run- time operation code image file.
filename	Name of the file or image. The file is not displayed if the file exists and contains errors.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

If you enter the dir command without any parameters, the system displays all files.

File information is shown below:

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
Size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
Console#dir
                        file name      file type startup size (byte)
 ------------------------------- -------------- ------- -----------
 Unit1:
                         Diag.bix Boot-Rom image       Y      818812
          ES4548C_ZZ(V0.1.0.2).bix Operation Code       Y     2346020
        Factory_Default_Config.cfg    Config File       N         374
                            startup    Config File       Y        7606
 ------------------------------------------------------------------
                                        Total free space:   3932160
Console#
```

16.27 disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

The following example shows executing the disable command.

```
Console#disable
Console>
```

Related Commands

enable

16.28 disconnect

Use this command to terminate an SSH, Telnet, or console connection.

Syntax Description

`disconnect session-id`

session-id	The session identifier for an SSH, Telnet or console connection. (Range: 0-4)

Command Mode

Privileged Exec

Usage Guidelines

Specifying session identifier “0” will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

The following example show disconnecting session 1.

```
Console#disconnect 1
Console#
```

Related Commands

show ssh

show users

16.29 dot1x default

This command sets all configurable dot1x global and port settings to their default values.

Syntax Description

`dot1x default`

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

16.30 dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the no form to restore the default.

Syntax Description

`dot1x max-req` *count*

no `dot1x max-req`

count	The maximum number of requests. (Range: 1-10)

Default

2

Command Mode

Global Configuration

Example

The following example shows setting the maximum number of requests to 2.

```
Console(config)#dot1x max-req 2
Console(config)#
```

16.31 dot1x operation-mode

This command allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. Use the no form without keywords to restore the default to single host. Use the no form with the multi-host max-count keywords to restore the default maximum count.

Syntax Description

`dot1x operation-mode {single-host | multi-host [max-count` *count*`]}`

no `dot1x operation-mode [multi-host max-count]`

single-host	Allows only a single host to connect to this port.
multi-host	Allows multiple host to connect to this port.
max-count	Keyword for the maximum number of hosts.
count	The maximum number of hosts that can connect to a port. (Range: 1-20; Default: 5)

Default

Single-host

Command Mode

Interface Configuration

Example

The following example shows setting the system to allow a maximum of 10 hosts to connect to a port.

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

16.32 dot1x port-control

This command sets the dot1x mode on a port interface. Use the no form to restore the default.

Syntax Description

```
dot1x port-control {auto | force-authorized | force-unauthorized}
```

```
no dot1x port-control
```

auto	Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
force-authorized	Configures the port to grant access to all clients.
force-unauthorized	Configures the port to deny access to all clients.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

16.33 dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

Syntax Description

```
dot1x re-authenticate [interface]
```

The interface argument includes Ethernet as follows:

unit	This is device 1.
port	Port number.

Command Mode

Privileged Exec

Example

```
Console#dot1x re-authenticate
Console#
```

16.34 dot1x re-authentication

This command enables periodic re-authentication globally for all ports. Use the no form to disable re-authentication.

Syntax Description

```
[no] dot1x re-authentication
```

Command Mode

Global Configuration

Example

```
Console(config)#dot1x re-authentication
Console(config)#
```

16.35 dot1x timeout quiet-period

This command sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the no form to reset the default.

Syntax Description

```
dot1x timeout quiet-period seconds

no dot1x timeout quiet-period
```

seconds	The number of seconds. (Range: 1-65535)

Default

60 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout quiet-period 350
Console(config)#
```

16.36 dot1x timeout re-authperiod

This command sets the period of time before a connected client must be re-authenticated.

Syntax Description

`dot1x timeout re-authperiod` *seconds*

no `dot1x timeout re-authperiod`

seconds	The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout re-authperiod 300
Console(config)#
```

16..37 dot1x timeout tx-period

This command sets the time that the switch waits during an authentication session before re-transmitting an EAP packet. Use the no form to reset to the default value.

Syntax Description

`dot1x timeout tx-period` *seconds*

no `dot1x timeout tx-period`

seconds	The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout tx-period 300
Console(config)#
```

16.38 enable

This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See section **14.5 Understanding Command Modes**.

Syntax Description

```
enable [level]
```

level	Privilege level to log into the device. The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default

Level 15

Command Mode

Normal Exec

Usage Guidelines

The default password required to change the command mode from Normal Exec to Privileged Exec is **super**. (To set this password, refer to the enable password command.

The "**#**" character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console>enable
Password: [privileged level password]
Console#
```

Related Commands

disable

enable password

16.39 enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the no form to reset the default password.

Syntax Description

```
enable password [level level] {0 | 7} password

no enable password [level level]
```

level level	Level 15 for Privileged Exec. (Levels 0 and 14 are not used.)
{0 | 7}	0 means plain password, 7 means encrypted password.
password	password for this privilege level. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default

The default is level 15.

The default password is “super”

Command Mode

Global Configuration

Usage Guidelines

You must enter a password to change the command mode from Normal Exec to Privileged Exec using the enable command.

The encrypted password is required for compatibility with legacy password settings (for example, plain or encrypted text) when reading the configuration file during initial system launch or when downloading the configuration file from a TFTP server. You do not need to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable

16.40 end

This command returns to Privileged Exec mode.

Default

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

16.41 exec-timeout

This command sets the interval that the system waits until user input is detected. Use the no form to restore the default.

Syntax Description

`exec-timeout [`*`seconds`*`]`

`no` `exec-timeout`

seconds	Integer that specifies the number of seconds. (Range: 0 - 65535 seconds; 0: no timeout)

Default

CLI: No timeout

Telnet: 10 minutes

Command

Line Configuration

Usage Guidelines

If user input is detected within the timeout interval, the session is kept open; otherwise, the session is terminated.

This command applies to both the local console and Telnet connections.

Telnet sessions cannot be disabled.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

16.42 exit

This command returns to the previous configuration mode or exit the configuration program.

Default

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session
User Access Verification

Username:
```

16.43 flowcontrol

This command enables flow control. Use the no form to disable flow control.

Syntax Description

```
[no] flowcontrol
```

Default

enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.

To force flow control on or off (with the flowcontrol or no flowcontrol command), use the no negotiation command to disable auto-negotiation on the selected interface.

When using the negotiation command to enable auto-negotiation, the optimal settings is determined by the capabilities command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port

Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise, back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation

capabilities (flowcontrol, symmetric)

16.44 garp timer

This command sets the values for the join, leave and leaveall timers. Use the no form to restore the timers' default values.

Syntax Description

`garp timer {join | leave | leaveall}` *`timer_value`*

`no` `garp timer {join | leave | leaveall}`

{join | leave | leaveall}	Which timer to set.
timer_value	Value of timer. Ranges: join: 20-1000 centiseconds leave: 60-3000 centiseconds leaveall: 500-18000 centiseconds

Default

join: 20 centiseconds

leave: 60 centiseconds

leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. Unless you are experiencing, difficulties with GMRP or GVRP registration/deregistration do not change timer values.

Timer values are applied to GVRP for all the ports on all VLANs.

Timer values must meet the following criteria:

- leave >= (2 x join)
- leaveall > leave

Note: To avoid problems set GVRP timers on all Layer 2 devices connected in the same network to the same values.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

show garp timer

16.45 hostname

This command specifies or modifies the host name for this device. Use the no form to restore the default host name.

Syntax Description

`hostname` *`name`*

`no` `hostname`

name	The name of this host. (Maximum length: 255 characters)

Default

None

Command Mode

Global Configuration

Example

The following example shows setting the host name to RD#1.

```
Console(config)#hostname RD#1
```

```
Console(config)#
```

16.46 interface

This command configures an interface type and enter interface configuration mode. Use the no form to remove a trunk.

Syntax Description

`interface` *`interface`*

`no` `interface port-channel channel-id`

interface	ethernet unit/port **unit** - This is device 1. **port** - Port number.
port-channel	channel-id (Range: 1-6)
Vlan	vlan-id (Range: 1-4094)

Default

None

Command Mode

Global Configuration

Example

To specify port 24, enter the following command:

```
Console(config)#interface ethernet 1/24
Console(config-if)#
```

16.47 interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.

Syntax Description

`interface vlan` *`vlan-id`*

vlan-id	ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

Default

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown

16.48 ip access-group

This command binds a port to an IP ACL. Use the no form to remove the port.

Syntax Description

[**no**] ip access-group *acl_name* {in | out}

acl_name	Name of the ACL. (Maximum length: 16 characters)
in	Indicates that this list applies to ingress packets.
out	Indicates that this list applies to egress packets.

Default

None

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

A port can only be bound to one ACL.

If a port is already bound to an ACL and you bind it to a different ACL, the switch replaces the old binding with the new one.

You must configure a mask for an ACL rule before you can bind it to a port.

Example

The following examples shows binding interface Ethernet 1/25 to IP access group david.

```
Console(config)#int eth 1/25
Console(config-if)#ip access-group david in
```

```
Console(config-if)#
```

Related Commands

show ip access-list

16.49 ip address

This command sets the IP address for the currently selected VLAN interface. Use the no form to restore the default IP address.

Syntax Description

```
ip address {ip-address netmask | bootp | dhcp}

no ip address
```

ip-address	IP address
netmask	Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
Bootp	Obtains IP address from BOOTP.
dhcp	Obtains IP address from DHCP.

Default

DHCP

Command Mode

Interface Configuration (VLAN)

Usage Guidelines

You must assign an IP address to this device to gain management access over the network. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Nothing outside this format will be accepted by the configuration program.

If you select the bootp or dhcp option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).

You can start broadcasting BOOTP or DHCP requests by entering an ip dhcp restart command, or by rebooting the switch.

Note: Before you change the IP address, you must first clear the current address with the no form of this command.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart

16.50 ip default-gateway

This command establishes a static route between this switch and management stations that exist on another network segment. Use the no form to remove the static route.

Syntax Description

`ip default-gateway` *gateway*

no `ip default-gateway`

gateway	IP address of the default gateway.

Default

No static route is established.

Command Mode

Global Configuration

Usage Guidelines

Define the gateway first if the management station is located in a different IP segment .

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

Related Commands

show ip redirects

16.51 ip dhcp restart

This command submits a BOOTP or DHCP client request.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

This command issues a BOOTP or DHCP client request for any IP interface set to BOOTP or DHCP mode using the ip address command.

DHCP requires the server to reassign the client's last address if available.

If the BOOTP or DHCP server was moved to a different domain, the network portion of the address provided to the client is based on this new domain.

Example

In the following example, the device is reassigned the same address and confirmed using the show interface command.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: Dhcp.
Console#
```

Related Commands

ip address

show ip interface

16.52 ip domain-list

This command defines a list of domain names that can be appended to incomplete host names (For example, host names passed from a client that are not formatted with dotted notation). Use the no form to remove a name from this list.

Syntax Description

[**no**] ip domain-list *name*

name	Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-64 characters)

Default

None

Command Mode

Global Configuration

Usage Guidelines

Domain names are added to the end of the list one at a time.

When an incomplete host name is received by the DNS server on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.

If there is no domain list, the domain name specified with the ip domain-name command is used. If there is a domain list, the default domain name is not used.

Example

This example adds two domain names to the current list and then displays the list and uses the show dns command to confirm the configuration.

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
Console#
```

Related Commands

ip domain-name

show dns

16.53 ip domain-lookup

This command enables DNS host name-to-address translation. Use the no form to disable DNS.

Syntax Description

[**no**] ip domain-lookup

Default

Disabled

Command Mode

Global Configuration

Usage Guidelines

At least one name server must be specified before you can enable DNS.

If all name servers are deleted, DNS is automatically disabled.

Example

This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Related Commands

ip domain-name

ip name-server

show dns

16.54 ip domain-name

This command defines the default domain name appended to incomplete host names (For example, host names passed from a client that are not formatted with dotted notation). Use the no form to remove the current domain name.

Syntax Description

`ip domain-name` *name*

no `ip domain-name`

name	Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-64 characters)

Default

None

Command Mode

Global Configuration

Example

```
Console(config)#ip domain-name sample.com
```

```
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    sample.com
Domain Name List:
Name Server List:
Console#
```

Related Commands

ip domain-list

ip name-server

ip domain-lookup

show dns

16.55 ip host

This command creates a static entry in the DNS table that maps a host name to an IP address. Use the no form to remove an entry.

Syntax Description

[**no**] ip host *name* address1 [address2 … address8]

name	Name of the host. (Range: 1-64 characters)
address1	Corresponding IP address.
address2 … address8	Additional corresponding IP addresses.

Default

No static entries

Command Mode

Global Configuration

Usage Guidelines

Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name using this command, a DNS client can try each address in succession, until it establishes a connection with the target device.

Example

This example maps two address to a host name and uses the show hosts commands to confirm configuration.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
```

```
Console(config)#end
Console#show hosts

Hostname
 rd5
Inet address
 192.168.1.55 10.1.0.55
Alias
Console#
```

Related Commands

show hosts

16.56 ip http port

This command specifies the TCP port number used by the Web browser interface. Use the no form to use the default port.

Syntax Description

`ip http port` *port-number*

no `ip http port`

port-number	The TCP port to be used by the browser interface. (Range: 1-65535)

Default

80

Command Mode

Global Configuration

Example

The following example shows setting the ip http port to 769.

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server

16.57 ip http secure-port

This command specifies the UDP port number used for HTTPS/SSL connection to the switch's Web interface. Use the no form to restore the default port.

Syntax Description

```
ip http secure-port port_number

no ip http secure-port
```

port_number	The UDP port used for HTTPS/SSL. (Range: 1-65535)

Default

443

Command Mode

Global Configuration

Usage Guidelines

You cannot configure HTTP and HTTPS servers to use the same port.

If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format:

```
https://device:port_number
```

Example

The following example shows setting the secure port to port 1000.

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server

16.58 ip http secure-server

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (For example, an encrypted connection) to the switch's Web interface. Use the no form to disable this function.

Syntax Description

```
[no] ip http secure-server
```

Default

Enabled

Command Mode

Global Configuration

Usage Guidelines

Both HTTP and HTTPS service can be enabled independently on the switch. You cannot configure the HTTP and HTTPS servers to use the same UDP port.

If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://device[:port_number]

When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server's digital certificate.
- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.

The client and server establish a secure encrypted connection.

A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x or later versions.

Jaci Verify this The following Web browsers and operating systems currently support HTTPS:

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

To specify a secure-site certificate, refer to the section **6.3.2 Replacing the Default Secure-site Certificate** and the **copy** command.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port

copy tftp https-certificate

16.59 ip http server

This command allows the device to be monitored or configured from a browser. Use the no form to disable this function.

Syntax Description

```
[no] ip http server
```

Default

Enabled

Command Mode

Global Configuration

Example

The following example shows setting the device to be monitored from the server.

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port

16.60 ip igmp snooping

This command enables IGMP snooping on this switch. Use the no form to disable it.

Syntax Description

```
[no] ip igmp snooping
```

Default

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

16.61 ip igmp snooping querier

This command enables the switch as an IGMP source that queries other IGMP hosts. Use the no form to disable it.

Syntax Description

```
[no] ip igmp snooping querier
```

Default

Enabled

Command Mode

Global Configuration

Usage Guidelines

If enabled, the switch serves as source that queries other hosts if elected. The switch is responsible for pinging hosts to receive multicast traffic connections.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

16.62 ip igmp snooping query-count

This command configures the query count. Use the no form to restore the default.

Syntax Description

`ip igmp snooping query-count` *count*

no `ip igmp snooping query-count`

count	The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

Default

2 times

Command Mode

Global Configuration

Usage Guidelines

The query count defines how long the IGMP query source waits for a response from a multicast client before taking action. If queries were sent and the client has not responded, a countdown timer is started using the time defined by ip igmp snooping query-max- response-time. If the countdown finishes, and the client still has not responded, then that client is no longer part of the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

ip igmp snooping query-max-response-time

16.63 ip igmp snooping query-interval

This command configures the query interval. Use the no form to restore the default.

Syntax Description

`ip igmp snooping query-interval` *seconds*

no `ip igmp snooping query-interval`

seconds	The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

16.64 ip igmp snooping query-max-response-time

This command configures the query report delay. Use the no form to restore the default.

Syntax Description

`ip igmp snooping query-max-response-time` *seconds*

no `ip igmp snooping query-max-response-time`

seconds	The report delay advertised in IGMP queries. (Range: 5-25)

Default

10 seconds

Command Mode

Global Configuration

Usage Guidelines

The switch must be using IGMPv2 for this command to take effect.

This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the ip igmp snooping query-count, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version

16.65 ip igmp snooping router-port-expire-time

This command configures the query timeout. Use the no form to restore the default.

Syntax Description

`ip igmp snooping router-port-expire-time` *seconds*

no `ip igmp snooping router-port-expire-time`

seconds	The time the switch waits before it considers the router port (for example, the interface which had been receiving query packets) to have expired. (Range: 300-500)

Default

300 seconds

Command Mode

Global Configuration

Usage Guidelines

The switch must use IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

Related Commands

ip igmp snooping version

16.66 ip igmp snooping version

This command configures the IGMP snooping version. Use the no form to restore the default.

Syntax Description

```
ip igmp snooping version {1 | 2}
```

```
no ip igmp snooping version
```

1	IGMP Version 1
2	IGMP Version 2

Default

IGMP Version 2

Command Mode

Global Configuration

Usage Guidelines

All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.

Some commands are only enabled for IGMPv2, including ip igmp query-max-response-time and ip igmp query-timeout.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

16.67 ip igmp snooping vlan mrouter

This command statically configures a multicast router port. Use the no form to remove the configuration.

Syntax Description

```
[no] ip igmp snooping vlan vlan-id mrouter interface
```

vlan-id	VLAN ID (Range: 1-4094)
interface	ethernet unit/port **unit** - This is device 1. **port** - Port number.

port-channel	channel-id (Range: 1-6)

Default

No static multicast router ports are configured.

Command Mode

Global Configuration

Usage Guidelines

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

16.68 ip igmp snooping vlan static

This command adds a port to a multicast group. Use the no form to remove the port.

Syntax Description

[**no**] ip igmp snooping vlan *vlan-id* static *ip-address interface*

vlan-id	VLAN ID (Range: 1-4094)
ip-address	IP address for multicast group
interface	ethernet unit/port **unit** - This is device 1. **port** - Port number.
port-channel	channel-id (Range: 1-6)

Default

None

Command Mode

Global Configuration

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

16.69 ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the no form to remove a name server from this list.

Syntax Description

```
[no] ip name-server server-address1 [server-address2 … server-address6]
```

server-address1	IP address of domain-name server.
server-address2 … server-address6	IP address of additional domain-name servers.

Default

None

Command Mode

Global Configuration

Usage Guidelines

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Example

This example adds two domain-name servers to the list and then displays the list. Use the show dns command to confirm configuration.

```
Console(config)#ip name-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Related Commands

ip domain-name

ip domain-lookup

show dns

16.70 ip ssh authentication-retries

Use this command to configure the number of times the SSH server attempts to reauthenticate a user. Use the no form to restore the default setting.

Syntax Description

`ip ssh authentication-retries` *count*

no `ip ssh authentication-retries`

count	The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default

3

Command Mode

Global Configuration

Example

The following example shows setting the SSH server to stop after the third attempt.

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh

16.71 ip ssh crypto host-key generate

Use this command to generate the host key pair (For example, public and private).

Syntax Description

`ip ssh crypto host-key generate [dsa | rsa]`

dsa	DSA (Version 2) key type.
rsa	RSA (Version 1) key type.

Default

Generates both

Command Mode

Privileged Exec

Usage Guidelines

This command stores the host key pair in memory (For example, RAM). Use the ip ssh save host-key command to save the host key pair to flash memory.

Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.

The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#
```

Related Commands

ip ssh crypto zeroize

ip ssh save host-key

16.72 ip ssh crypto zeroize

Use this command to clear the host key from memory (For example RAM).

Syntax Description

```
ip ssh crypto zeroize [dsa | rsa]
```

dsa	DSA (Version 2) key type.
rsa	RSA (Version 1) key type.

Default

Clears both

Command Mode

Privileged Exec

Usage Guidelines

This command clears the host key from volatile memory (RAM). Use the no ip ssh save host-key command to clear the host key from flash memory.

The SSH server must be disabled before you can execute this command.

Example

```
Console#ip ssh crypto zeroize dsa
Console#
```

Related Commands

ip ssh crypto host-key generate

ip ssh save host-key

no ip ssh server

16.73 ip ssh save host-key

Use this command to save host key from RAM to flash memory.

Syntax Description

```
ip ssh save host-key
```

Default

Save

Command Mode

Privileged Exec

Example

```
Console#ip ssh save host-key
Console#
```

Related Commands

ip ssh crypto host-key generate

16.74 ip ssh server

Use this command to enable the Secure Shell (SSH) server on this switch. Use the no form to disable this service.

Syntax Description

```
ip ssh server
```

no ip ssh server

Default

Disabled

Command Mode

Global Configuration

Usage Guidelines

The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

You must generate the host key before enabling the SSH server.

Example

```
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

ip ssh crypto host-key generate

show ssh

16.75 ip ssh server-key size

Use this command to set the SSH server key size. Use the no form to restore the default setting.

Syntax Description

ip ssh server-key size *key-size*

no ip ssh server-key size

key-size	The size of server key. (Range: 512-896 bits)

Default

768 bits

Command Mode

Global Configuration

Usage Guidelines

The server key is a private key that is never shared outside the switch.

The host key is shared with the SSH client, and is fixed at 1024 bits.

Example

The following example shows setting the private key to 512.

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

16.76 ip ssh timeout

Use this command to configure the timeout for the SSH server. Use the no form to restore the default setting.

Syntax Description

`ip ssh timeout` *seconds*

no `ip ssh timeout`

seconds	The timeout for client response during SSH negotiation. (Range: 1-120)

Default

10 seconds

Command Mode

Global Configuration

Usage Guidelines

The timeout specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the exec-timeout command for vty sessions.

Example

The following example show setting the session to time out after 1 minute.

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

exec-timeout

show ip ssh

16.77 jumbo frame

This command enables support for jumbo frames. Use the no form to disable it.

Syntax Description

```
[no] jumbo frame
```

Default

Disabled

Command Mode

Global Configuration

Usage Guidelines

This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. In addition, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. For half-duplex connections, all devices in the collision domain would need to support jumbo frames.

Enabling jumbo frames limits the maximum threshold for broadcast storm control to 64 packets per second. (See the **switchport broadcast** command.)

Example

```
Console(config)#jumbo frame
Console(config)#
```

16.78 lacp

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the no form to disable it.

Syntax Description

```
[no] lacp
```

Default

Disabled

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.

If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.

If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 11-13. Because LACP has also been enabled on the ports at the other end of the links, the show interfaces status port-channel 1 command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 1000T
  Mac address: 00-00-e8-00-00-0b
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
  Port security: Disabled
  Max MAC count: 0
 Current status:
  Created by: lacp
  Link status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/11, Eth1/12, Eth1/13,
Console#
```

Related Command

show interfaces

16.79 lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the no form to restore the default setting.

Syntax Description

```
lacp {actor | partner} admin-key key

[no] lacp {actor | partner} admin-key
```

actor	The local side an aggregate link.
partner	The remote side of an aggregate link.
key	The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

Default

0

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel admin key matches (if configured).

If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (For example, it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.

Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

16.80 lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the no form to restore the default setting.

Syntax Description

```
lacp admin-key key

[no] lacp admin-key
```

key	Use the port channel admin key to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)

Default

0

Command Mode

Interface Configuration (Port Channel)

Usage Guidelines

Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).

If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (For example, it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

Example

```
Console(config)#interface port channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

16.81 lacp port-priority

This command configures LACP port priority. Use the no form to restore the default setting.

Syntax Description

`lacp {actor | partner} port-priority` *priority*

no `lacp {actor | partner} port-priority`

actor	Use this to set the local side an aggregate link.
partner	Use this to set the remote side of an aggregate link.
priority	Use this to set the LACP port priority to select a backup link. (Range: 0-65535)

Default

32768

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

Setting a lower value indicates a higher effective priority.

If an active port link goes down, the backup port with the highest priority replaces the downed link. If two or more ports have the same LACP port priority, the port with the lowest physical port number is used as the backup port.

Once the remote side of a link is established, LACP operational settings are in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and only takes effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

16.82 lacp system-priority

This command configures a port's LACP system priority. Use the no form to restore the default setting.

Syntax Description

`lacp {actor | partner} system-priority` *priority*

no `lacp {actor | partner} system-priority`

actor	Use this to set the local side an aggregate link.
partner	Use this to set the remote side of an aggregate link.
priority	Use this to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default

32768

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

You must configure the port with the same system priority to join the same LAG.

The system priority combined with the switch's MAC address forms the LAG identifier. This identifier indicates the specific LAG during LACP negotiations with other systems.

When the remote side of a link is established, LACP operational settings are in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

16.83 line

This command identifies a specific line for configuration, and to process subsequent line configuration commands.

Syntax Description

```
line {console | vty}
```

console	Console terminal line.
vty	Virtual terminal for remote console access (For example, Telnet).

Default

There is no default line.

Command Mode

Global Configuration

Usage Guidelines

Telnet is a virtual terminal connection and is shown as “Vty” in screen displays such as show users. The serial communication parameters (for example databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line

show users

16.84 logging facility

This command sets the facility type for remote logging of syslog messages. Use the no form to return the type to the default.

Syntax Description

```
[no] logging facility type
```

type	A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default

23

Command Mode

Global Configuration

Usage Guidelines

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. It may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
Console(config)#logging facility 19
Console(config)#
```

16.85 logging history

This command limits syslog messages saved to switch memory based on severity. The no form returns the logging of syslog messages to the default level.

Syntax Description

`logging history {flash | ram}` *`level`*

`no` `logging history {flash | ram}`

flash	Event history stored in flash memory (For example, permanent memory).
ram	Event history stored in temporary RAM (For example, memory flushed on power reset).
level	One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

The following table gives information on each level name, number and general description.

Level Name	Level	Description
debugging	7	Debugging messages
informational	6	Informational messages only
notifications	5	Normal but significant condition, such as cold start
warnings	4	Warning conditions (such as, return false, unexpected return)
Errors	3	Error conditions (such as, invalid input, default used)

critical	2	Critical conditions (such as, memory allocation, or free memory error - resource exhausted)
Alerts	1	Immediate action needed
emergencies	0	System unusable

Note: Error messages are only at Level 2, 5 and 6.

Default

Flash: errors (level 3 - 0)

RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Usage Guidelines

The message level specified for flash memory must be a higher priority (for example, numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

16.86 logging host

This command adds a syslog server host IP address that will receive logging messages. Use the no form to remove a syslog server host.

Syntax Description

[**no**] logging host *host_ip_address*

host_ip_address	The IP address of a syslog server.

Default

None

Command Mode

Global Configuration

Usage Guidelines

Use this command more than once to build a list of host IP addresses.

The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

16.87 logging on

This command controls logging of error messages, sending debug or error messages to switch memory. The no form disables the logging process.

Syntax Description

```
[no] logging on
```

Default

None

Command Mode

Global Configuration

Usage Guidelines

The logging process controls error messages saved to switch memory. You can use the logging history command to control the type of error messages that are stored.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history

clear logging

16.88 logging sendmail

This command enables SMTP event handling. Use the no form to disable this function.

Syntax Description

```
[no] logging sendmail
```

Default

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail
Console(config)#
```

16.89 logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the no form to remove a recipient.

Syntax Description

[**no**] logging sendmail destination-email *email-address*

Email-address	The source email address used in alert messages. (Range: 1-41 characters)

Default

None

Command Mode

Global Configuration

Usage Guidelines

You can specify up to five recipients for alert messages. To do this, you must enter a separate command to specify each recipient.

Example

```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

16.90 logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the no form to remove an SMTP server.

Syntax Description

[**no**] logging sendmail host *ip_address*

ip_address	IP address of an SMTP server that will be sent alert messages for event handling.

Default

None

Command Mode

Global Configuration

Usage Guidelines

You can specify up to three SMTP servers for event handing. You must enter a separate command to specify each server.

To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.

To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

16.91 logging sendmail level

This command sets the severity threshold used to trigger alert messages.

Syntax Description

`logging sendmail level` *`level`*

level	One of the system message levels. Messages sent include the selected level down to level 0. (Range: 0-7) For more information on the levels, refer to the table in logging history command.

Default

Level 7

Command Mode

Global Configuration

Usage Guidelines

The specified level indicates an event threshold. All events at this level or higher are sent to the configured email recipients. (For example, using Level 7 reports all events from level 7 to level 0.)

Example

This example shows setting the system to send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```

16.92 logging sendmail source-email

This command sets the email address used for the “From” field in alert messages.

Syntax Description

```
logging sendmail source-email email-address
```

Email-address	The source email address used in alert messages. (Range: 1-41 characters)

Default

None

Command Mode

Global Configuration

Usage Guidelines

You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

This example shows setting to system to send email alerts for system alerts for emails received from a specific address.

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

16.93 logging trap

This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the no form to disable remote logging.

Syntax Description

```
logging trap [level]

no logging trap
```

level	One of the level arguments listed in the table under the logging history command. Messages sent include the selected level up through level 0.

Default

Level 3 - 0

Command Mode

Global Configuration

Example

```
Console(config)#logging trap 4
Console(config)#
```

16.94 login

This command enables password checking at login. Use the no form to disable password checking and allow connections without a password.

Syntax Description

`login [local]`

no login

Local	Selects local password checking. Authentication is based on the user name specified with the username command.

Default

login local

Command Mode

Line Configuration

Usage Guidelines

There are three authentication modes provided at login:

Login	Selects authentication by a single global password as specified by the password line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
login local	Selects authentication via the user name and password specified by the username command (For example, default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
no login	Selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

This command controls login authentication through the switch. To configure user names and passwords for remote authentication servers, use the RADIUS or TACACS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username

password

16.95 mac access-group

This command binds a port to a MAC ACL. Use the no form to remove the port.

Syntax Description

`mac access-group` *`acl_name`* `{in | out}`

acl_name	Name of the ACL. (Maximum length: 16 characters)
In	Indicates that this list applies to ingress packets.
Out	Indicates that this list applies to egress packets.

Default

None

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

A port can only be bound to one ACL.

If a port is already bound to an ACL and you bind it to a different ACL, the switch replaces the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/25
Console(config-if)#mac access-group james in
Console(config-if)#
```

Related Commands

show mac access-list

16.96 mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the no form to restore the default aging time.

Syntax Description

`mac-address-table aging-time` *`seconds`*

`no` `mac-address-table aging-time`

Seconds	Aging time. (Range: 10-1000000 seconds; 0 to disable aging)

Default

300 seconds

Command Mode

Global Configuration

Usage Guidelines

Use this command to dynamically delete learned forwarding information after a specified period of time.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

16.97 mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the no form to remove an address.

Syntax Description

`mac-address-table static` *`mac-address`* `interface` *`interface`* `vlan` *`vlan-id`* `[action]`

`no` `mac-address-table static` *`mac-address`* `vlan` *`vlan-id`*

mac-address	The MAC address.
interface	Is ethernet unit/port **unit** - This is device 1. **port** - Port number.
port-channel	channel-id (Range: 1-6)
vlan-id	VLAN ID (Range: 1-4094)
Action	Specify delete-on-reset - Assignment lasts until the switch is reset. permanent - Assignment is permanent

Default

no

The default mode is permanent.

Command Mode

Global Configuration

Usage Guidelines

You can define the static address for a host device to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

Static addresses remain in the address table if the interface link is down.

Static addresses are bound to the assigned interface. When a static address is detected on another interface, the address is ignored and not added to the address table.

Static addresses are not added until the address is removed by using the no form of this command.

Example

The following is sample output from the mac-address-table command using the static argument.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
1/1 vlan 1 delete-on-reset
```

16.98 management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the no form to restore the default setting.

Syntax Description

[**no**] management {all-client | http-client | snmp-client | telnet-client} *start-address* [*end-address*]

all-client	Adds IP address(es) to the SNMP, Web and Telnet groups.
http-client	Adds IP address(es) to the Web group.
snmp-client	Adds IP address(es) to the SNMP group.
telnet-client	Adds IP address(es) to the Telnet group.
Start-address	A single IP address, or the starting address of a range.
end-address	The end address of a range.

Default

All addresses

Command Mode

Global Configuration

Usage Guidelines

If anyone tries to access a management interface on the switch from an invalid address, the switch rejects the connection, enter an event message in the system log, and send a trap message to the trap manager.

IP address can be configured for SNMP, Web and Telnet access respectively. Each of these groups can either include up to five different sets of addresses, individual addresses or address ranges.

When entering addresses for the same group (For example, SNMP, Web or Telnet), the switch does not accept overlapping address ranges. When entering addresses for different groups, the switch accepts overlapping address ranges.

You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.

You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

Related Commands

show management

16.99 map access-list ip

This command sets the output queue for packets matching an ACL rule. The specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. Use the no form to remove the CoS mapping.

Syntax Description

[**no**] map access-list ip *acl_name* cos *cos-value*

acl_name	Name of the ACL. (Maximum length: 16 characters)
cos-value	CoS value. (Range: 0-7)

Default

None

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

You must configure an ACL mask before you can map CoS values to the rule.

A packet matching a rule within the specified ACL is mapped to one of the output queues as shown in the following table. For information on mapping the CoS values to output queues, see **queue cos-map** command.

Priority	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Queue	1	2	0	3	4	5	6	7

Example

```
Console(config)#interface ethernet 1/25
Console(config-if)#map access-list ip david cos 0
Console(config-if)#
```

Related Commands

queue cos-map

show map access-list ip

16.100 mask (IP ACL)

This command defines a mask for IP ACLs. This mask defines the fields to check in the IP header. Use the no form to remove a mask.

Syntax Description

[**no**] mask [protocol]

{any | *host* | *source-bitmask*}

{any | host | *destination-bitmask*}

[precedence] [tos] [dscp]

[source-port [*port-bitmask*]] [destination-port [*port-bitmask*]]

[control-flag [*flag-bitmask*]]

protocol	Check the protocol field.
any	Any address will be matched.
host	The address must be for a host device, not a subnetwork.
source-bitmask	Source address of rule must match this bitmask.
destination-bitmask	Destination address of rule must match this bitmask.
precedence	Check the IP precedence field.
tos	Check the TOS field.
dscp	Check the DSCP field.

source-port	Check the protocol source port field.
destination-port	Check the protocol destination port field.
port-bitmask	Protocol port of rule must match this bitmask. (Range: 0-65535)
control-flag	Check the field for control flags.
flag-bitmask	Control flags of rule must match this bitmask. (Range: 0-63)

Default

None

Command Mode

IP Mask

Usage Guidelines

Use this command to check packets crossing a port against the rules set in the ACL until it finds a match. The order the rules entered in the ACL file do not determine the order the packets are checked.

You must first create the required ACLs and ingress or egress masks before mapping an ACL to an interface.

If you enter dscp, you cannot enter tos or precedence. You can enter both tos and precedence without dscp.

Masks that include an entry for a Layer 4 protocol source port or destination port only apply to packets with a header length of exactly five bytes.

Example

This example creates an IP ingress mask with two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the “deny 10.1.1.1 255.255.255.255” rule has the higher precedence according the “mask host any” entry.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

This shows how to create a standard ACL with an ingress mask to deny access to the IP host 171.69.198.102, and permit access to any others.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit any
Console(config-std-acl)#deny host 171.69.198.102
Console(config-std-acl)#end
Console#show access-list
IP standard access-list A2:
  deny host 171.69.198.102
  permit any
Console#configure
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A2 in
Console(config-if)#end
Console#show access-list
IP standard access-list A2:
  deny host 171.69.198.102
  permit any
Console#
```

This shows how to create an extended ACL with an egress mask to drop packets leaving network 171.69.198.0 when the Layer 4 source port is 23.

```
Console(config)#access-list ip extended A3
Console(config-ext-acl)#deny host 171.69.198.5 any
Console(config-ext-acl)#deny 171.69.198.0 255.255.255.0 any source-port 23
Console(config-ext-acl)#end
Console#show access-list
IP extended access-list A3:
  deny host 171.69.198.5 any
  deny 171.69.198.0 255.255.255.0 any source-port 23
Console#config
Console(config)#access-list ip mask-precedence out
Console(config-ip-mask-acl)#mask 255.255.255.0 any source-port
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/15
Console(config-if)#ip access-group A3 out
Console(config-if)#end
Console#show access-list
IP extended access-list A3:
  deny 171.69.198.0 255.255.255.0 any source-port 23
  deny host 171.69.198.5 any
IP egress mask ACL:
  mask 255.255.255.0 any source-port
Console#
```

This is a more comprehensive example. It denies any TCP packets in which the SYN bit is ON, and permits all other packets. It then sets the ingress mask to check the deny rule first, and finally binds port 1 to this ACL. Note that once the ACL is bound to an interface (For example, the ACL is active), the order in which the rules are displayed is determined by the associated mask.

```
Switch(config)#access-list ip extended A6
```

```
Switch(config-ext-acl)#permit any any
Switch(config-ext-acl)#deny tcp any any control-flag 2 2
Switch(config-ext-acl)#end
Console#show access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
Console#configure
Switch(config)#access-list ip mask-precedence in
Switch(config-ip-mask-acl)#mask protocol any any control-flag 2
Switch(config-ip-mask-acl)#end
Console#sh access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#configure
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A6 in
Console(config-if)#end
Console#show access-list
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

16.101 map access-list mac

This command sets the output queue for packets matching an ACL rule. The specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. Use the no form to remove the CoS mapping.

Syntax Description

[**no**] map access-list mac *acl-name* cos *cos-value*

acl-name	Name of the ACL. (Maximum length: 16 characters)
cos-value	CoS value. (Range: 0-7)

Default

None

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

You must configure an ACL mask before you can map CoS values to the rule.

A packet matching a rule within the specified ACL then maps to one of the output queues as shown below.

Priority	0	1	2	3	4	5	6	7
Queue	1	2	0	3	4	5	6	7

Example

```
Console(config)#int eth 1/5
Console(config-if)#map access-list mac M5 cos 0
Console(config-if)#
```

Related Commands

queue cos-map

show map access-list mac

16.102 map ip dscp (Global Configuration)

This command enables IP DSCP mapping (For example, Differentiated Services Code Point mapping). Use the no form to disable IP DSCP mapping.

Syntax Description

```
[no] map ip dscp
```

Default

Disabled

Command Mode

Global Configuration

Usage Guidelines

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

16.103 map ip dscp (Interface Configuration)

This command sets IP DSCP priority (For example, Differentiated Services Code Point priority). Use the no form to restore the default table.

Syntax Description

`map ip dscp` *`dscp-value`* `cos` *`cos-value`*

`no` `map ip dscp`

dscp-value	DSCP value. (Range: 0-63)
cos-value	Class-of-Service value (Range: 0-7)

Default

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.

This command sets the IP DSCP priority for all interfaces.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

16.104 map ip port (Global Configuration)

This command enables IP port mapping (For example, class of service mapping for TCP/UDP sockets). Use the no form to disable IP port mapping.

Syntax Description

[**no**] map ip port

Default

Disabled

Command Mode

Global Configuration

Usage Guidelines

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

Example

The following example shows how to enable TCP/UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```

16.105 map ip port (Interface Configuration)

This command enables IP port mapping (For example, TCP/UDP port priority). Use the no form to remove a specific setting.

Syntax Description

map ip port *port number* cos *cos-value*

no map ip port *port-number*

port-number	The 16-bit TCP/UDP port number.(Range 1-65535)
cos-value	The Class-of-Service value. (Range: 0-7)

Default

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

This command sets the IP port priority for all interfaces.

Example

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

16.106 map ip precedence (Global Configuration)

This command enables IP precedence mapping (for example, IP Type of Service). Use the no form to disable IP precedence mapping.

Syntax Description

[**no**] map ip precedence

Default

Disabled

Command Mode

Global Configuration

Usage Guidelines

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

16.107 map ip precedence (Interface Configuration)

This command sets IP precedence priority (For example, IP Type of Service priority). Use the no form to restore the default table.

Syntax Description

map ip precedence *ip-precedence-value* cos *cos-value*

no map ip precedence

precedence-value	3-bit precedence value. (Range: 0-7)

cos-value	Class-of-Service value (Range: 0-7)

Default

The list below shows the default priority mapping.

IP Precedence Value	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
CoS Value	0	1	2	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.

This command sets the IP Precedence for all interfaces.

Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

16.108 mask (MAC ACL)

This command defines a mask for MAC ACLs. This mask defines the fields to check in the packet header. Use the no form to remove a mask.

Syntax Description

[**no**] mask [pktformat]

{any | host | *source-bitmask*} {any | host | *destination-bitmask*}

[vid [*vid-bitmask*]] [ethertype [*ethertype-bitmask*]]

pktformat	Check the packet format field. (If this keyword is used in the mask, the packet format must be specified in ACL rule to match.)
any	Match any address.
host	The address must be for a single node.

source-bitmask	Source address of rule must match this bitmask.
destination-bitmask	Destination address of rule must match this bitmask.
vid	Check the VLAN ID field.
vid-bitmask	VLAN ID of rule must match this bitmask.
Ethertype	Check the Ethernet type field.
ethertype-bitmask	Ethernet type of rule must match this bitmask.

Default

None

Command Mode

MAC Mask

Usage Guidelines

Up to seven masks can be assigned to an ingress or egress ACL.

Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.

Create the required ACLs and inbound or outbound masks before mapping an ACL to an interface.

Example

This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4
Console(config-mac-acl)#permit any any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11 ff-ff-ff-ff-ff-ff
any vid 3
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M4:
  permit any any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#mac access-group M4 in
Console(config-if)#end
Console#show access-list
MAC access-list M4:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
  permit any any
MAC ingress mask ACL:
  mask pktformat host any vid
```

```
Console#
```

This example creates an Egress MAC ACL.

```
Console(config)#access-list mac M5
Console(config-mac-acl)#deny tagged-802.3 host 00-11-11-11-11-11 any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11 ff-ff-ff-ff-ff-ff
any vid 3 ethertype 0806
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M5:
  deny tagged-802.3 host 00-11-11-11-11-11 any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
Console#configure
Console(config)#access-list mac mask-precedence out
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#mac access-group M5 out
Console(config-if)#end
Console#show access-list
MAC access-list M5:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
  deny tagged-802.3 host 00-11-11-11-11-11 any
MAC ingress mask ACL:
  mask pktformat host any vid ethertype
Console#
```

16.109 match access-list ip

This command changes the IEEE 802.1p priority, IP Precedence, or DSCP Priority of a frame matching the defined ACL rule. (This feature is commonly referred to as ACL packet marking.) Use the no form to remove the ACL marker.

Syntax Description

`match access-list ip` *`acl_name`* `[set priority` *`priority`*`] {set precedence` *`precedence_value`* `| set dscp` *`dscp_value`*`}`

`no` `match access-list ip` *`acl_name`*

acl_name	Name of the ACL. (Maximum length: 16 characters)
priority	Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest)
precedence_value	IP Precedence value. (Range: 0-7)
dscp_value	Differentiated Services Code Point value. (Range: 0-63)

Default

None

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

You must configure an ACL mask before you can change frame priorities based on an ACL rule.

Traffic priorities may be included in the IEEE 802.1p priority tag. This tag is also incorporated as part of the overall IEEE 802.1Q VLAN tag. To specify this priority, use the set priority keywords.

The IP frame header also includes priority bits in the Type of Service (ToS) octet. The Type of Service octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. To specify the IP precedence priority, use the set tos keywords. To specify the DSCP priority, use the set dscp keywords. The IP frame header can include either the IP Precedence or DSCP priority type.

The precedence for priority mapping by this switch is IP Precedence or DSCP Priority, and then 802.1p priority.

Example

```
Console(config)#interface ethernet 1/12
Console(config-if)#match access-list ip bill set dscp 0
Console(config-if)#
```

Related Commands

show marking

16.110 match access-list mac

This command changes the IEEE 802.1p priority of a Layer 2 frame matching the defined ACL rule. (This feature is commonly referred to as ACL packet marking.) Use the no form to remove the ACL marker.

Syntax Description

`match access-list mac` *`acl_name`* `set priority` *`priority`*

`no` `match access-list mac` *`acl_name`*

acl_name	Name of the ACL. (Maximum length: 16 characters)
priority	Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest)

Default

None

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

You must configure an ACL mask before you can change frame priorities based on an ACL rule.

Example

```
Console(config)#interface ethernet 1/12
Console(config-if)#match access-list mac james set priority 0
Console(config-if)#
```

Related Commands

show marking

16.111 max-hops

This command configures the maximum number of hops in the region before a BPDU is discarded. Use the no form to restore the default.

Syntax Description

`max-hops` *hop-number*

hop-number	Maximum hop number for multiple spanning tree. (Range: 1-40)

Default

20

Command Mode

MST Configuration

Usage Guidelines

A MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside a MSTI region is never changed. Each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that propagates a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Example

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

16.112 mst priority

This command configures the priority of a spanning tree instance. Use the no form to restore the default.

Syntax Description

`mst` *`instance_id`* `priority` *`priority`*

`no` `mst` *`instance_id`* `priority`

instance_id	Instance identifier of the spanning tree. (Range: 0-64)
priority	Priority of the a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default

32768

Command Mode

MST Configuration

Usage Guidelines

MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (For example, lowest numerical value) becomes the MSTI root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device.

You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

Example

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

16.113 mst vlan

This command adds VLANs to a spanning tree instance. Use the no form to remove the specified VLANs. Using the no form without any VLAN parameters to remove all VLANs.

Syntax Description

[**`no`**] `mst` *`instance_id`* `vlan` *`vlan-range`*

instance_id	Instance identifier of the spanning tree. (Range: 0-4094)
vlan-range	Range of VLANs. (Range: 1-4094)

Default

none

Command Mode

MST Configuration

Usage Guidelines

Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default, all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 58 instances. You should try to group VLANs that cover the same general area of your network. You must configure all bridges within the same MSTI Region (see the **name** command) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

Example

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

16.114 name

This command configures the name for the multiple spanning tree region in which this switch is located. Use the no form to clear the name.

Syntax Description

`name` *name*

name	Name of the spanning tree.

Default

Switch's MAC address

Command Mode

MST Configuration

Usage Guidelines

Use the MST region name and revision number (refer to the mst command) to designate a unique MST region. A bridge (for example, spanning-tree compliant device such as this switch) can only belong to one MST region and all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

Related Commands

revision

16.115 negotiation

This command enables auto-negotiation for a specified interface. Use the no form to disable a previously set auto-negotiation.

Syntax Description

[**no**] negotiation

Default

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

When auto-negotiation is enabled, the switch negotiates the best settings for a link based on the capabilities command. When auto-negotiation is disabled, you must manually specify the link attributes with the speed-duplex and flowcontrol commands.

If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration is also disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

capabilities

flowcontrol

speed-duplex

16.116 parity

This command defines the generation of a parity bit. Use the no form to restore the default setting.

Syntax Description

parity {none | even | odd}

no parity

none	No parity
even	Even parity
odd	Odd parity

Default

no parity

Command Mode

Line Configuration

Usage Guidelines

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify even parity, enter this command:

```
Console(config-line)#parity even
Console(config-line)#
```

16.117 password

This command specifies the password for a line. Use the no form to remove the password.

Syntax Description

`password {0 | 7} password`

no password

{0 | 7}	0 means plain password, 7 means encrypted password
password	Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default

No password is specified.

Command Mode

Line Configuration

Usage Guidelines

When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the password-thresh command to

set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.

The encrypted password is required for compatibility with legacy password settings (For example, plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login

password-thresh

16.118 password-thresh

This command sets the password intrusion threshold, which limits the number of failed logon attempts. Use the no form to remove the threshold value.

Syntax Description

`password-thresh [threshold]`

no `password-thresh`

threshold	The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default

The default is three attempts.

Command Mode

Line Configuration

Usage Guidelines

When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent-time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.

This command applies to both the local console and Telnet connections.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time

16.119 permit, deny (Extended ACL)

This command adds a rule to an Extended IP ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the no form to remove a rule.

Syntax Description

```
[no] {permit | deny} [protocol-number | udp]
{any | source address-bitmask | host source}
{any | destination address-bitmask | host destination}
[precedence precedence] [tos tos] [dscp dscp]
[source-port sport [bitmask]] [destination-port dport [port-bitmask]]
[no] {permit | deny} tcp
{any | source address-bitmask | host source}
{any | destination address-bitmask | host destination}
[precedence precedence] [tos tos] [dscp dscp]
[source-port sport [bitmask]] [destination-port dport [port-bitmask]]
[control-flag control-flags flag-bitmask]
```

protocol-number	A specific protocol number. (Range: 0-255)
source	Source IP address.
destination	Destination IP address.
address-bitmask	Decimal number representing the address bits to match.
host	Keyword followed by a specific IP address.
precedence	IP precedence level. (Range: 0-7)
tos	Type of Service level. (Range: 0-7)
dscp	DSCP priority level. (Range: 0-63)
sport	Protocol* source port number. (Range: 0-65535)
dport	Protocol (Includes TCP, UDP or other protocol types) destination port number. (Range: 0-65535)

port-bitmask	Decimal number representing the port bits to match. (Range: 0-65535)
control-flags	Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
flag-bitmask	Decimal number representing the code bits to match. (Range: 0-63)

Default

None

Command Mode

Extended ACL

Usage Guidelines

All new rules are appended to the end of the list.

Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

You can specify both Precedence and ToS in the same rule. If DSCP is used, then neither Precedence nor ToS can be specified.

The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:

- 1 (fin) – Finish
- 2 (syn) – Synchronize
- 4 (rst) – Reset
- 8 (psh) – Push
- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

SYN flag valid, use “control-code 2 2”

Both SYN and ACK valid, use “control-code 18 18”

SYN valid and ACK invalid, use “control-code 2 18”

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; For example, the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (For example, HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port
80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any control-flag 2
2
Console(config-ext-acl)#
```

Related Commands

access-list ip

16.120 permit, deny (MAC ACL)

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (For example, physical layer address), or Ethernet protocol type. Use the no form to remove a rule.

Syntax Description

[**no**] {permit | deny}

{any | host source | source *address-bitmask*}

{any | host *destination* | destination *address-bitmask*}

[vid *vid vid-bitmask*] [ethertype *protocol* [*protocol-bitmask*]]

Note: - The default is for Ethernet II packets.

[**no**] {permit | deny} tagged-eth2

[ethertype *protocol* [*protocol-bitmask*]]

[**no**] {permit | deny} tagged-802.3

tagged-eth2	Tagged Ethernet II packets.
untagged-eth2	Untagged Ethernet II packets.
tagged-802.3	Tagged Ethernet 802.3 packets.
untagged-802.3	Untagged Ethernet 802.3 packets.
any	Any MAC source or destination address.

host	A specific MAC address.
source	Source MAC address.
destination	Destination MAC address range with bitmask.
address-bitmask	Bitmask for MAC address (in hexadecimal format)) (1 means care and 0 means ignore).
vid	VLAN ID. (Range: 1-4095).
vid-bitmask	VLAN bitmask. (Range: 1-4095) (1 means care and 0 means ignore).
protocol	A specific Ethernet protocol number. (Range: 600-fff hex.)
protocol-bitmask	Protocol bitmask. (Range: 600-fff hex.) (1 means care and 0 means ignore).

Default

None

Command Mode

MAC ACL

Usage Guidelines

New rules are added to the end of the list.

The ethertype option can only be used to filter Ethernet II formatted packets.

A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:

- 0800 - IP
- 0806 - ARP
- 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

Related Commands

access-list mac

16.121 permit, deny (Standard ACL)

This command adds a rule to a Standard IP ACL. The rule sets a filter condition for packets emanating from the specified source. Use the no form to remove a rule.

Syntax Description

[**no**] {permit | deny} {any | *source bitmask* | host *source*}

any	Any source IP address.
source	Source IP address.
bitmask	Decimal number representing the address bits to match.
host	Keyword followed by a specific IP address.

Default

None

Command Mode

Standard ACL

Usage Guidelines

New rules are appended to the end of the list.

Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Related Commands

access-list ip

16.122 ping

This command sends ICMP echo request packets to another node on the network.

Syntax Description

ping *host* [size *size*] [count *count*]

host	IP address or IP alias of the host.
size	Number of bytes in a packet. (Range: 32-512, default: 32) The actual packet size will be eight bytes larger than the size specified because the switch adds header information.
count	Number of packets to send. (Range: 1-16, default: 5)

Default

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

Use the ping command to see if another site on the network can be reached. Press <Esc> to stop pinging.

Following are some results of the ping command:

Normal response	The normal response occurs in one to ten seconds, depending on network traffic.
Destination does not respond	If the host does not respond, a “timeout” appears in ten seconds.
Destination unreachable	The gateway for this destination indicates that the destination is unreachable.
Network or host unreachable	The gateway found no corresponding entry in the route table.

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface

16.123 port security

This command enables or configures port security. Use the no form without any keywords to disable port security. Use the no form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax Description

`port security [action {shutdown | trap | trap-and-shutdown} | max-mac-count address-count]`

no `port security [action | max-mac-count]`

action	Response to take when port security is violated. **shutdown** - Disable port only. **trap** - Issue SNMP trap message only. **trap-and-shutdown** - Issue SNMP trap message and disable port.
max-mac-count	The maximum number of MAC addresses that can be counted on a port. (Range: 0 - 20)
address-count	The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 20)

Default

Status: Disabled

Action: None

Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

If you enable port security, the switch stops dynamically learning new addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table are accepted.

To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port.

To add new VLAN members at a later time, you can manually add secure addresses with the mac-address-table static command, or turn off port security to re-enable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.

A secure port has the following restrictions:

- Cannot use port monitoring.

- Cannot be a multi-VLAN port.
- Cannot be connected to a network interconnection device.
- Cannot be a trunk port.

If a port is disabled due to a security violation, it must be manually re-enabled using the no shutdown command.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

Related Commands

shutdown

mac-address-table static

show mac-address-table

16.124 prompt

This command customizes the CLI prompt. Use the no form to restore the default prompt.

Syntax Description

`prompt` *`string`*

`no` `prompt`

string	Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default

Console

Command Mode

Global Configuration

Example

```
Console(config)#prompt RD2
RD2(config)#
Console(config)#
```

16.125 protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the no form to remove a protocol group.

Syntax Description

`protocol-vlan protocol-group` *`group-id`* `[{add | remove}` *`frame_type`* `frame protocol-type` *`protocol`*`]`

`no` `protocol-vlan protocol-group` *`group-id`*

group-id	Group identifier of this protocol group. (Range: 1-2147483647)
frame	Frame type used by this protocol. (Options: ethernet, rfc_1042, llc_other)
protocol	Protocol type. The only option for the llc_other frame type is ipx_raw. The options for all other frames types include: ip, arp, rarp.

Default

No protocol groups are configured.

Command Mode

Global Configuration

Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
protocol-type arp
Console(config)#
```

16.126 protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the no form to remove the protocol mapping for this interface.

Syntax Description

`protocol-vlan protocol-group` *`group-id`* `vlan` *`vlan-id`*

`no` `protocol-vlan protocol-group` *`group-id`* `vlan`

group-id	Group identifier of this protocol group. (Range: 1-2147483647)
vlan-id	VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

Default

No protocol groups are mapped for any interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (see **15.14.2**), these interfaces will admit traffic of any protocol type into the associated VLAN.

When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:

- If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
- If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
- If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Example

The following example maps the traffic entering Port 1, which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

16.127 pvlan

This command enables or configures a private VLAN. Use the no form to disable the private VLAN.

Syntax Description

pvlan [up-link *interface-list* down-link *interface-list*]

no pvlan

up-link	Specifies an uplink interface.
down-link	Specifies a downlink interface.

Default

No private VLANs are defined.

Command Mode

Global Configuration

Usage Guidelines

A private VLAN provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the uplink port.

Private VLANs and normal VLANs can exist simultaneously within the same switch.

Entering the pvlan command without any parameters enables the private VLAN. Entering no pvlan disables the private VLAN.

Example

This example enables the private VLAN, and then sets port 24 as the uplink and ports 1-4 as the downlinks.

```
Console(config)#pvlan
Console(config)#pvlan up-link ethernet 1/24 down-link ethernet 1/1-4
```

16.128 queue bandwidth

This command assigns weighted round-robin (WRR) weights to the eight class of service (CoS) priority queues. Use the no form to restore the default weights.

Syntax Description

queue bandwidth *weight1...weight4*

no queue bandwidth

weight1...weight4	The ratio of weights for queues 0 - 3 determines the weights used by the WRR scheduler. (Range: 1 - 15)

Default

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

WRR controls bandwidth sharing at the egress port by defining scheduling weights.

Example

This example shows how to assign WRR weights to each of the priority queues:

```
Console(config)#interface ethernet 1/8
Console(config-if)#queue bandwidth 1 3 5 7 9 11 13 15
Console(config-if)#
```

Related Commands

show queue bandwidth

16.129 queue cos-map

This command assigns class of service (CoS) values to the priority queues (For example, hardware output queues 0 - 7). Use the no form set the CoS map to the default values.

Syntax Description

`queue cos-map` *`queue_id`* `[cos1 ... cosn]`

`no` `queue cos-map`

queue_id	The ID of the priority queue. Ranges are 0 to 7, where 7 is the highest priority queue.
cos1 .. cosn	The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default

This switch supports Class of Service by using eight priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown below.

Queue	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Priority	2	0	1	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

CoS values assigned at the ingress port are also used at the egress port.

This command sets the CoS priority for all interfaces.

Example

The following example shows how to change the CoS assignments to a one-to-one mapping:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 Cos Value     : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Console#
```

Related Commands

show queue cos-map

16.130 queue mode

This command sets the queue mode to strict priority or Weighted Round-Robin (WRR) for the class of service (CoS) priority queues. Use the no form to restore the default value.

Syntax Description

```
queue mode {strict | wrr}

no queue mode
```

strict	Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
wrr	Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 - 7 respectively.

Default

Weighted Round Robin

Command Mode

Global Configuration

Usage Guidelines

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use WRR queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

16.131 quit

This command exits the configuration program.

Default

None

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

The quit and exit commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

16.132 radius-server host

This command specifies the RADIUS server. Use the no form to restore the default.

Syntax Description

`radius-server host` *host_ip_address*

no `radius-server host`

host_ip_address	IP address of server.

Default

10.1.0.1

Command Mode

Global Configuration

Example

```
Console(config)#radius-server host 192.168.1.25
Console(config)#
```

16.133 radius-server key

This command sets the RADIUS encryption key. Use the no form to restore the default.

Syntax Description

`radius-server key` *key_string*

no radius-server key

key_string	Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

16.134 radius-server port

This command sets the RADIUS server network port. Use the no form to restore the default.

Syntax Description

radius-server port *port_number*

no radius-server port

port_number	RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

16.135 radius-server retransmit

This command sets the number of retries. Use the no form to restore the default.

Syntax Description

radius-server retransmit *number_of_retries*

no radius-server retransmit

number_of_retries	Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

16.136 radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the no form to restore the default.

Syntax Description

`radius-server timeout` *`number_of_seconds`*

`no` `radius-server timeout`

number_of_seconds	Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

16.137 rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the no form to restore the default status of disabled.

Syntax Description

`rate-limit {input | output} [`*`rate`*`]`

no rate-limit {input | output}

input	Input rate
output	Output rate
rate	Maximum value in Mbps. (Range: 1 to 1000 Mbps)

Default

1000 Mbps

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 600
Console(config-if)#
```

16.138 reload

This command restarts the system.

Note: When the system is restarted, it runs the Power-On Self-Test. It retains all configuration information stored in non-volatile memory by the copy running-config startup-config command.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

16.139 revision

This command configures the revision number for this multiple spanning tree configuration of this switch. Use the no form to restore the default.

Syntax Description

`revision` *`number`*

number	Revision number of the spanning tree. (Range: 0-65535)

Default

0

Command Mode

MST Configuration

Usage Guidelines

The MST region name and revision number are used to designate a unique MST region. A bridge (for example, spanning-tree compliant device such as this switch) can only belong to one MST region. In addition, all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

Related Commands

name

16.140 show access-group

This command shows the port assignments of ACLs.

Command Mode

Privileged Executive

Example

The following is sample output from the show access-group command.

```
Console#show access-group
Interface ethernet 1/25
 IP standard access-list james
 MAC access-list jerry
Console#
```

16.141 show access-list

This command shows all ACLs and associated rules, as well as all the user-defined masks.

Command Mode

Privileged Exec

Usage Guidelines

Once the ACL is bound to an interface (for example, the ACL is active), the order in which the rules are displayed is determined by the associated mask.

Example

The following is sample output from the show access-list command.

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
IP extended access-list bob:
  permit 10.7.1.1 0.0.0.255 any
  permit 192.168.1.0 0.0.0.255 any dport 80
  permit 192.168.1.0 0.0.0.255 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any 00-30-29-94-34-de ethertype 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

16.142 show access-list ip mask-precedence

This command shows the ingress or egress rule masks for IP ACLs.

Syntax Description

```
show access-list ip mask-precedence [in | out]
```

in	Ingress mask precedence for ingress ACLs.
out	Egress mask precedence for egress ACLs.

Command Mode

Privileged Exec

Example

The following is sample output from the show access-list ip mask precedence command.

```
Console#show access-list ip mask-precedence
IP ingress mask ACL:
  mask host any
  mask 255.255.255.0 any
Console#
```

Related Commands

mask (IP ACL)

16.143 show access-list mac mask-precedence

This command shows the ingress or egress rule masks for MAC ACLs.

Syntax Description

show access-list mac mask-precedence [in | out]

in	Ingress mask precedence for ingress ACLs.
out	Egress mask precedence for egress ACLs.

Command Mode

Privileged Exec

Example

The following is sample output from the show access-list mac mask-precedence command.

```
Console#show access-list mac mask-precedence
MAC egress mask ACL:
  mask pktformat host any vid ethertype
Console#
```

Related Commands

mask (MAC ACL)

16.144 show bridge-ext

This command shows the configuration for bridge extension commands.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

See section **10.1.3 Displaying Basic VLAN Information** and section **2.10.4 Displaying Bridge Extension Capabilities** for a description of the displayed items.

Example

The following is sample output from the show bridge-ext command.

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

16.145 show calendar

This command displays the system clock.

Default

None

Command Mode

Normal Exec, Privileged Exec

Example

The following is sample output from the show calendar command.

```
Console#show calendar
 15:12:34 February 1 2004
Console#
```

16.146 show dns

This command displays the configuration of the DNS server.

Command Mode

Privileged Exec

Example

The following is sample output from the show dns command.

```
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
```

```
    10.1.0.55
Console#
```

16.147 show dns cache

This command displays entries in the DNS cache.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show dns cache command.

```
Console#show dns cache
NO       FLAG    TYPE    IP              TTL     DOMAIN
0         4      CNAME   10.2.44.96      893     pttch_pc.accton.com.tw
1         4      CNAME   10.2.44.3       898     ahten.accton.com.tw
2         4      CNAME   66.218.71.84    298     www.yahoo.akadns.net
3         4      CNAME   66.218.71.83    298     www.yahoo.akadns.net
4         4      CNAME   66.218.71.81    298     www.yahoo.akadns.net
5         4      CNAME   66.218.71.80    298     www.yahoo.akadns.net
6         4      CNAME   66.218.71.89    298     www.yahoo.akadns.net
7         4      CNAME   66.218.71.86    298     www.yahoo.akadns.net
8         4      ALIAS   POINTER TO:7    298     www.yahoo.com
Console#
```

Field	Description
NO	The entry number for each resource record.
FLAG	The flag is always “4” indicating a cache entry and therefore unreliable.
TYPE	This field includes CNAME which specifies the canonical or primary name for the owner, and ALIAS which specifies multiple domain names, which are mapped to the same IP address as an existing entry.
IP	The IP address associated with this record.
TTL	The time to live reported by the name server.
DOMAIN	The domain name associated with this record.

16.148 show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

Syntax Description

`show dot1x [statistics] [interface` *`interface`*`]`

interface	ethernet unit/port • unit - This is device 1. • port - Port number.

Command Mode

Privileged Exec

Usage Guidelines

This command displays the following information:

Global 802.1X Parameters – Displays the global port access control parameters that can be configured for this switch as described in the preceding pages, including **reauth-enabled**, **reauth-period**, **quiet-period**, **tx-period** and **max-req** commands. It also displays the following global parameters that are set to a fixed value, including the following items:

supp-timeout	Supplicant timeout.
server-timeout	Server timeout.
reauth-max	Maximum number of reauthentication attempts.
802.1X Port Summary	Displays the port access control parameters for each interface, including the following items:
Status	Administrative state for port access control.
Operation Mode	**Dot1x port operation mode** command.
Mode	**Dot1x port control mode** command.
Authorized	Authorization status (yes or n/a - not authorized).
802.1X Port Details	Displays detailed port access control settings for each interface as described in the preceding pages, including **dot1x operation mode**, **dot1x max count**, **dot1x port-control** and **dot1x current Identifier** commands. It also displays the following information:
Status	Authorization status (authorized or unauthorized).
Supplicant	MAC address of authorized client.

Authenticator State Machine

State	Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
Reauth Count	Number of times connecting state is re-entered.

Backend State Machine

State	Current state (including request, response, success, fail, timeout, idle, initialize).
Request Count	Number of EAP Request packets sent to the Supplicant without receiving a response.
Identifier(Server)	Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

Reauthentication State Machine

State	Current state (including initialize, reauthenticate).

Example

The following is sample output from the show dot1x command.

```
Console#show dot1x  Global 802.1X Parameters
 reauth-enabled: yes
 reauth-period:  3600
 quiet-period:   60
 tx-period:      30
 supp-timeout:   30
 server-timeout: 30
 reauth-max:     2
 max-req:        2

802.1X Port Summary
 Port Name     Status     Operation Mode                Mode     Authorized
       1/1   disabled        Single-Host      ForceAuthorized            n/a
       1/2   disabled        Single-Host      ForceAuthorized            n/a
.
.
.
      1/47   disabled        Single-Host      ForceAuthorized            n/a
      1/48   enabled         Single-Host                Auto             yes

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is disabled on port 1/2
.
.
.
.

802.1X is disabled on port  1/47

802.1X is enabled on port  1/48
Status              Authorized
Operation mode      Single-Host
Max count           5
Port-control        Auto
```

```
Supplicant          00-00-e8-49-5e-dc
Current Identifier  3

Authenticator State Machine
State               Authenticated
Reauth Count        0

Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  2

Reauthentication State Machine
State               Initialize
Console#
```

16.149 show garp timer

This command shows the GARP timers for the selected interface.

Syntax Description

```
show garp timer [interface]
```

interface	ethernet unit/port • unit - This is device 1. • port - Port number.
port-channel	channel-id (Range: 1-6)

Default

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

The following is sample output from the show garp timer command.

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer: 20 centiseconds
 Leave timer: 60 centiseconds
 Leaveall timer: 1000 centiseconds
Console#
```

Related Commands

garp timer

16.150 show gvrp configuration

This command shows if GVRP is enabled.

Syntax Description

```
show gvrp configuration [interface]
```

interface	ethernet unit/port • unit - This is device 1. • port - Port number.
port-channel	channel-id (Range: 1-6)

Default

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

The following is sample output from the show gvrp configuration command .

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 Gvrp configuration: Disabled
Console#
```

16.151 show history

This command shows the contents of the command history buffer.

Default

None

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

The following is sample output from the show history command.

```
Console#show history
```

```
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The ! command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the !2 command repeats the second command in the Execution history buffer (config).

```
Console#!2
Console#config
Console(config)#
```

16.152 show hosts

This command displays the static host name-to-address mapping table.

Command Mode

Privileged Exec

Example

The following is sample output from the show hosts command.

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
Console#
```

16.153 show interfaces counters

This command displays interface statistics.

Syntax Description

```
show interfaces counters [interface]
```

interface	ethernet unit/port (source port) unit - Switch (unit 1). port - port number
port-channel	channel-id (Range: 1-6)

Default

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see section **7.8 Showing Port Statistics**.

Example

The following is sample output from the show interfaces counters command .

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/7
 Iftable stats:
  Octets input: 30658, Octets output: 196550
  Unicast input: 6, Unicast output: 5
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 3064
  Broadcast input: 262, Broadcast output: 1
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 227208, Packets: 3338
  Broadcast pkts: 263, Multi-cast pkts: 3064
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
  Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

16.154 show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

Syntax Description

```
show interfaces protocol-vlan protocol-group [interface]
```

interface

interface	ethernet unit/port • unit - This is device 1. • port - Port number.
port-channel	channel-id (Range: 1-6)

Default

The mapping for all interfaces is displayed.

Command Mode

Privileged Exec

Example

The following is sample output from the show interfaces protocol-vlan protocol-group command.

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group

   Port     ProtocolGroup ID    Vlan ID
---------- ------------------ -----------
   Eth 1/1                  1       vlan2
Console#
```

16.155 show interfaces status

This command displays the status for an interface.

Syntax Description

```
show interfaces status [interface]
```

interface	ethernet unit/port unit – This is device 1. port - Port number.

port-channel	Channel-id (Range: 1-6)
vlan	Vlan-id (Range: 1-4094)

Default

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see section **7.1 Displaying Connection Status**.

Example

The following is sample output from the show interfaces status command.

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
 Basic information:
  Port type: 1000T
  Mac address: 00-00-AB-CD-00-01
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
Current status:
  Link status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
Console#show interfaces status vlan 1
 Information of VLAN 1
 MAC address: 00-00-A3-42-00-80
Console#
```

16.156 show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

Syntax Description

```
show interfaces switchport [interface]
```

interface	Ethernet unit/port (source port) unit - Switch (unit 1). port - Port number.
port-channel	channel-id (Range: 1-6)

Default

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

If no interface is specified, information on all interfaces is displayed.

Example

The following is sample output from the show interfaces switchport command .

This example shows the configuration setting for port 24.

```
Console#show interfaces switchport ethernet 1/24
 Broadcast threshold: Enabled, 500 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,1000M bits per second
 Egress rate limit: disable,1000M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

Field	Description
Broadcast threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level.
Lacp status	Shows if Link Aggregation Control Protocol has been enabled or disabled.
Ingress/Egress rate limit	Shows if rate limiting is enabled, and the current rate limit.
VLAN membership mode	Indicates membership mode as Trunk or Hybrid.
Ingress rule	Shows if ingress filtering is enabled or disabled.

Acceptable frame type	Shows if acceptable VLAN frames include all types or tagged frames only.
Native VLAN	Indicates the default Port VLAN ID.
Priority for untagged traffic	Indicates the default priority for untagged frames.
Gvrp status	Shows if GARP VLAN Registration Protocol is enabled or disabled.
Allowed Vlan	Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged.
Forbidden Vlan	Shows the VLANs this interface can not dynamically join via GVRP.

16.157 show ip access-group

This command shows the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

The following is sample output from the show ip access-group command.

```
Console#show ip access-group
Interface ethernet 1/25
 IP access-list david in
Console#
```

Related Commands

ip access-group

16.158 show ip access-list

This command displays the rules for configured IP ACLs.

Syntax Description

`show ip access-list {standard | extended} [acl_name]`

standard	Specifies a standard IP ACL.
extended	Specifies an extended IP ACL.
acl_name	Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

The following is sample output from the show ip access-list command.

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
Console#
```

Related Commands

permit, deny

ip access-group

16.159 show ip igmp snooping

This command shows the IGMP snooping configuration.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

See section **12.1.1 Configuring IGMP Snooping and Query Parameters** for a description of the displayed items.

Example

The following is sample output from the show ip igmp snooping command.

```
Console#show ip igmp snooping
 Service status: Enabled
 Querier status: Enabled
 Query count: 2
 Query interval: 125 sec
 Query max response time: 10 sec
 Router port expire time: 300 sec
 IGMP snooping version: Version 2
Console#
```

16.160 show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

Syntax Description

`show ip igmp snooping mrouter [vlan` *`vlan-id`*`]`

vlan-id	VLAN ID (Range: 1-4094)

Default

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Usage Guidelines

Multicast router port types displayed include Static or Dynamic.

Example

The following is sample output from the show ip igmp snooping mrouter command.

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN  M'cast Router Port  Type
 ---- ------------------- -------
    1            Eth 1/11  Static
    2            Eth 1/12  Dynamic
Console#
```

16.161 show ip interface

This command displays the settings of an IP interface.

Default

All interfaces

Command Mode

Privileged Exec

Example

The following is sample output from the show ip interface command.

```
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Related Commands

show ip redirects

16.162 show ip redirects

This command shows the default gateway configured for this device.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show ip redirects command.

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway

16.163 show ip ssh

Use this command to display the connection settings used when authenticating client access to the SSH server.

Command Mode

Privileged Exec

Example

The following is sample output from the show ip ssh command.

```
Console#show ip ssh
SSH Enabled - version 1.99
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```

16.164 show lacp

This command displays LACP information.

Syntax Description

`show lacp [port-channel] {counters | internal | neighbors | sysid}`

port-channel	Local identifier for a link aggregation group. (Range: 1-6)

counters	Statistics for LACP protocol messages.
internal	Configuration settings and operational state for local side.
neighbors	Configuration settings and operational state for remote side.
sysid	Summary of system priority and MAC address for all channel groups.

Default

Port Channel: all

Command Mode

Privileged Exec

Example

The following is sample output from the show lacp command.

```
Console#show lacp 1 counters
Channel group : 1 -------------------------------------------------------------
------------
Eth 1/ 1 ----------------------------------------------------------------------
---
  LACPDUs Sent : 21
  LACPDUs Received : 21
  Marker Sent : 0
  Marker Received : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
.
.
.
```

The following table describes fields shown in the show lacp counter display.

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```
Console#show lacp 1 internal
Channel group : 1
------------------------------------------------------------------------
Oper Key : 4
Admin Key : 0
Eth 1/1
------------------------------------------------------------------------
  LACPDUs Internal : 30 sec
  LACP System Priority : 32768
  LACP Port Priority : 32768
  Admin Key : 4
  Oper Key : 4
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State : distributing, collecting, synchronization, aggregation,
               long timeout, LACP-activity
.
.
.
```

The following table describes fields shown in the show lacp internal display.

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin or Oper State	Administrative or operational vales of the actor's parameters. Expired – The actor's receive machine is in the expired state; Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. Distributing – If false, distribution of outgoing frames on this link is disabled; For example, distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. Collecting – Collection of incoming frames on this link is enabled; For example, collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. Synchronization – The System considers this link to be IN_SYNC; For example, it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted.

	Aggregation – The system considers this link to be aggregatable; For example, a potential candidate for aggregation. Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

```
Console#show lacp 1 neighbors
Channel group 1 neighbors
-------------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------------
  Partner Admin System ID : 32768, 00-00-00-00-00-00
  Partner Oper System ID : 32768, 00-00-00-00-00-01
  Partner Admin Port Number : 1
  Partner Oper Port Number : 1
  Port Admin Priority : 32768
  Port Oper Priority : 32768
  Admin Key : 0
  Oper Key : 4
  Admin State : defaulted, distributing, collecting, synchronization,
                long timeout,
  Oper State : distributing, collecting, synchronization, aggregation,
               long timeout, LACP-activity
.
.
.
```

The following table describes fields shown in the show lacp neighbor display.

Field	**Description**
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)

Oper State	Operational values of the partner's state parameters. (See preceding table.)

The following is sample output from the show lacp sysid command.

```
Console#show lacp sysid
Channel group    System Priority    System MAC Address
--------------------------------------------------------------------------
            1              32768     00-30-F1-8F-2C-A7
            2              32768     00-30-F1-8F-2C-A7
            3              32768     00-30-F1-8F-2C-A7
            4              32768     00-30-F1-8F-2C-A7
            5              32768     00-30-F1-8F-2C-A7
            6              32768     00-30-F1-8F-2C-A7
Console#
```

The following table describes fields shown in the show lacp sysid display.

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority	LACP system priority for this channel group. The LACP system priority and system MAC address are concatenated to form the LAG system ID.
System MAC Address	System MAC address. The LACP system priority and system MAC address are concatenated to form the LAG system ID.

16.165 show line

This command displays the terminal line's parameters.

Syntax Description

`show line [`*`console`* `|` *`vty`*`]`

Console	Console terminal line.
Vty	Virtual terminal for remote console access (for example, Telnet).

Default

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

The following is sample output from the show line command.

```
Console#show line
 Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 600 sec
Console#
```

16.166 show logging

This command displays the logging configuration, along with any system and event messages stored in memory.

Syntax Description

```
show logging {flash | ram | sendmail | trap}
```

Flash	Event history stored in flash memory (For example, permanent memory).
Ram	Event history stored in temporary RAM (For example, memory flushed on power reset).
Sendmail	Displays settings for the SMTP event handler.
trap	Displays settings for the trap function.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show logging command.

This example shows that system logging is enabled, the message level for flash memory is “errors” (For example, default level 3 - 0), the message level for RAM is “debugging” (For example, default level 7 - 0).

```
Console#show logging flash
Syslog logging: Enable
History logging in FLASH: level errors
```

```
Console#
```

The following table show logging output.

Field	Description
Syslog logging	Shows if system logging has been enabled via the logging on command.
History logging in FLASH	The message level(s) reported based on the logging history command.
History logging in RAM	The message level(s) reported based on the logging history command.

The following example displays settings for the trap function.

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type: Debugging messages
REMOTELOG server IP address: 1.2.3.4
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#
```

The following table show logging traps output.

Field	Description
Syslog logging	Shows if system logging has been enabled via the logging on command.
REMOTELOG status	Shows if remote logging has been enabled via the logging trap command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the logging facility command.
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the logging trap command.
REMOTELOG server IP address	The address of syslog servers as specified in the logging host command.

Related Commands

show logging sendmail

16.167 show logging sendmail

This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, Privileged Exec

Example

The following is sample output from the show logging sendmail command .

```
Console#show logging sendmail
SMTP servers
------------------------------------------------

Active SMTP server: 192.168.1.19

SMTP minimum severity level: 7

SMTP destination email addresses
------------------------------------------------
 1. ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enable

Console#
```

16.168 show mac access-group

This command shows the ports assigned to MAC ACLs.

Command Mode

Privileged Exec

Example

The following is sample output from the show mac access-group command .

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 out
Console#
```

Related Commands

mac access-group

16.169 show mac access-list

This command displays the rules for configured MAC ACLs.

Syntax Description

```
show mac access-list [acl_name]
```

acl_name	Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

The following is sample output from the show mac access-list command.

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

Related Commands

permit, deny

mac access-group

16.170 show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

Syntax Description

`show mac-address-table [address` *`mac-address`* `[mask]] [interface` *`interface`*`] [vlan` *`vlan-id]`* `[sort {address | vlan | interface}]`

mac-address	MAC address.
mask	Bits to match in the address.
interface	ethernet unit/port unit - This is device 1. port - Port number.
port	channel channel-id (Range: 1-6)
vlan-id	VLAN ID (Range: 1-4094)
sort	Sort by address, vlan or interface.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:

- Learned - Dynamic address entries
- Permanent - Static entry
- Delete-on-reset - Static entry to be deleted when system is reset

The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit "0" means to match a bit and "1" means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."

The maximum number of address entries is 8191.

Example

The following is sample output from the show mac-address-table command.

```
Console#show mac-address-table
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de    1 Delete-on-reset
Console#
```

16.171 show mac-address-table aging-time

This command shows the aging time for entries in the address table.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show mac-address-table aging-time command.

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

16.172 show mac-address-table multicast

This command shows known multicast addresses.

Syntax Description

`show mac-address-table multicast [vlan` *`vlan-id`*`] [user | igmp-snooping]`

vlan- id	VLAN ID (1 to 4094)
user	Display only the user configured multicast entries.
Igmp- snooping	Display only entries learned through IGMP snooping.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

Member types displayed include IGMP or USER, depending on selected options.

Example

The following is sample output from the mac-address-table command with the multicast argument.

This shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/11    IGMP
Console#
```

16.173 show map access-list ip

This command shows the CoS value mapped to an IP ACL for the current interface. (The CoS value determines the output queue for packets matching an ACL rule.)

Syntax Description

```
show map access-list ip [interface]
```

interface	ethernet unit/port unit - This is device 1. port - Port number.

Command Mode

Privileged Exec

Example

The following is sample output from the show map access-list ip command.

```
Console#show map access-list ip
Eth 1/25
 access-list ip david cos 0
Console#
```

Related Commands

map access-list ip

16.174 show map access-list mac

This command shows the CoS value mapped to a MAC ACL for the current interface. (The CoS value determines the output queue for packets matching an ACL rule.)

Syntax Description

`show map access-list mac [interface]`

interface	ethernet unit/port • unit - This is device 1. • port - Port number.

Command Mode

Privileged Exec

Example

The following is sample output from the show map access-list mac command.

```
Console#show map access-list mac
Access-list to COS of Eth 1/5
 Access-list M5 cos 0
Console#
```

Related Commands

map access-list mac

16.175 show map ip dscp

This command shows the IP DSCP priority map.

Syntax Description

`show map ip dscp [interface]`

interface	ethernet unit/port unit - This is device 1.

	port - Port number. port-channel channel-id (Range: 1-6)

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show map ip dscp command with the argument.

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
.
.
.
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Related Commands

map ip dscp (Global Configuration)

map ip dscp (Interface Configuration)

16.176 show map ip port

This command shows the IP port priority map.

Syntax Description

`show map ip port [`*`interface`*`]`

interface	ethernet unit/port • unit - This is device 1. • port - Port number. port-channel channel-id (Range: 1-6)

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show map ip port command.

The example shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port ethernet 1/5
TCP port mapping status: enabled

 Port       Port no.  COS
 --------- ---------- ---
  Eth 1/ 5         80   0
Console#
```

Related Commands

map ip port (Global Configuration)

map ip port (Interface Configuration)

16.177 show map ip precedence

This command shows the IP precedence priority map.

Syntax Description

```
show map ip precedence [interface]
```

interface	ethernet unit/port • unit - This is device 1. • port - Port number. port-channel channel-id (Range: 1-6)

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show map ip precedence command.

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
```

```
  Eth 1/ 5          0   0
  Eth 1/ 5          1   1
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

Related Commands

map ip port (Global Configuration)

map ip precedence (Interface Configuration)

16.178 show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax Description

```
show management {all-client | http-client | snmp-client | telnet-
client}
```

all-client	Adds IP address(es) to the SNMP, Web and Telnet groups.
http-client	Adds IP address(es) to the Web group.
snmp-client	Adds IP address(es) to the SNMP group.
telnet-client	Adds IP address(es) to the Telnet group.

Command Mode

Privileged Exec

Example

The following is sample output from the show management command.

```
Console#show management all-client
Management Ip Filter
 Http-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 Snmp-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30
```

```
 Telnet-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```

Related Commands

Management

16.179 show marking

This command displays the current configuration for packet marking.

Command Mode

Privileged Exec

Example

The following is sample output from the show marking command.

```
Console#show marking
Interface ethernet 1/12
 match access-list IP bill set DSCP 0
 match access-list MAC a set priority 0
Console#
```

Related Commands

match access-list ip

16.180 show port monitor

This command displays mirror information.

Syntax Description

`show port monitor [interface]`

interface-ethernet	unit/port (source port) unit - Switch (unit 1).
port	Port number.

Default

Shows all sessions.

Command Mode

Privileged Exec

Usage Guidelines

This command displays the currently configured source port, destination port, and mirror mode (For example, RX, TX, RX/TX).

Example

The following is sample output from the show port monitor command.

The example shows mirroring configured from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/1
 Source port(monitored port)  :Eth1/6
 Mode                         :RX/TX
Console#
```

16.181 show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

Syntax Description

`show protocol-vlan protocol-group [group-id]`

group- id	Group identifier for a protocol group. (Range: 1-2147483647)

Default

All protocol groups are displayed.

Command Mode

Privileged Exec

Example

The following is sample output from the show protocol-vlan protocol-group command.

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

 ProtocolGroup ID   Frame Type    Protocol Type
------------------ ------------- ---------------
                1      ethernet     08 00
```

```
Console#
```

16.182 show public-key

Use this command to show the public key for the specified user or for the host.

Syntax Description

```
show public-key [user [username]| host]
```

username	Name of an SSH user. (Range: 1-8 characters)

Default

Shows all public keys.

Command Mode

Privileged Exec

Usage Guidelines

If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.

When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

The following is sample output from the show public-key command.

```
Console#show public-key host
Host:
RSA:
1024 35
156849954018676692593339467750546173253136748908365472541502024559319986854435836
361651999923329781766065830958610825913212890233765468017262725714134287629413011
196195566782595664104869574278881462065194174677298486546861571773939016477935594
230357741309802273708779454524083971752646358058176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv
JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbvwrNL
aQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7 w0W
Console#
```

16.183 show pvlan

This command displays the configured private VLAN.

Command Mode

Privileged Exec

Example

The following is sample output from the show pvlan command.

```
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/24
Down-link port:
 Ethernet 1/1
 Ethernet 1/2
 Ethernet 1/3
 Ethernet 1/4
Console#
```

16.184 show queue bandwidth

This command displays the weighted round-robin (WRR) bandwidth allocation for the eight priority queues.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show queue bandwidth command.

```
Console#show queue bandwidth
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
    0        1
    1        2
    2        4
    3        6
    4        8
    5        10
    6        12
    7        14
.
.
.
Console#
```

16.185 show queue cos-map

This command shows the class of service priority map.

Syntax Description

```
show queue cos-map [interface]
```

interface	ethernet unit/port unit - This is device 1. port - Port number. port-channel channel-id (Range: 1-6)

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show queue cos-map command.

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value     : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Console#
```

16.186 show queue mode

This command shows the current queue mode.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show queue mode command.

```
Console#show queue mode

Queue mode: strict
Console#
```

16.187 show radius-server

This command displays the current settings for the RADIUS server.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show radius-server command.

```
Console#show radius-server
Server IP address: 10.1.0.1
 Communication key with radius server:
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#
```

16.188 show running-config

This command displays the configuration information currently in use.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

Use this command in conjunction with the show startup-config command to compare the information in running memory to the information stored in non-volatile memory.

This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:

- SNMP community strings
- Users (names, access levels, and encrypted passwords)
- VLAN database (VLAN ID, name and state)
- VLAN configuration settings for each interface
- Multiple spanning tree instances (name and interfaces)
- IP address configured for VLANs

- Spanning tree settings
- Any configured settings for the console port and Telnet

Example

The following is sample output from the show running-config command.

```
Console#show running-config
building running-config, please wait.....
!
phymap 00-00-a3-42-00-80
!
sntp server 0.0.0.0 0.0.0.0 0.0.0.0
sntp client
sntp broadcast client
sntp poll 60
!
snmp-server community private rw
snmp-server community public ro
!
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
!
logging sendmail destination-email ted
logging sendmail source-email bill
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
.
.
!
spanning-tree mst-configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
.
.
.
!
interface vlan 1
 ip address 10.1.0.1 255.255.255.0
!
!
no spanning-tree
!
!
no ip igmp snooping
!
no map ip precedence
no map ip dscp
!
```

```
line console
!
line vty
!
end
Console#
```

Related Commands

show startup-config

16.189 show snmp

This command checks the status of SNMP communications.

Default

None

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the snmp-server enable traps command.

Example

The following is sample output from the show snmp command.

```
Console#show snmp

System Contact: Paul
System Location: WC-19

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. alpha, and the privilege is read-write
   2. private, and the privilege is read-write
   3. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
```

```
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP logging: enabled
    Logging to 10.1.19.23 batman version 1
Console#
```

16.190 show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

This command displays the current time, the poll interval used for sending time synchronization requests (when the switch is set to SNTP client mode), and the current SNTP mode (For example, client or broadcast).

Example

The following is sample output from the show sntp command.

```
Console#show sntp
Current time:  Jul 10 05:13:28 2003
Poll interval: 16
Current mode:  broadcast
Console#
```

16.191 show spanning-tree

This command shows the configuration for the common spanning tree (CST) or for an instance within the multiple spanning tree (MST).

Syntax Description

`show spanning-tree [`*`interface`* `|` `mst` *`instance_id`*`]`

interface	ethernet unit/port • unit - This is device 1. • port - Port number. port-channel channel-id (Range: 1-6)
instance_id	Instance identifier of the multiple spanning tree. (Range: 0-4094, no leading

	zeroes)

Default

None

Command Mode

Privileged Exec

Usage Guidelines

Use the show spanning-tree command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.

Use the show spanning-tree interface command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).

Use the show spanning-tree mst instance_id command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST).

For a description of the items displayed under “Spanning-tree information,” see **Chapter 3: Configuring Global Settings**. For a description of the items displayed for specific interfaces, refer to section **3.1.5 Displaying Interface Settings**.

Example

The following is sample output from the show spanning-tree command.

```
Console#show spanning-tree
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode               :MSTP
 Spanning tree enable/disable     :enable
 Instance                         :0
 Vlans configuration              :1-4094
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Max hops                         :20
 Remaining hops                   :20
 Designated Root                  :32768.0.0000ABCD0000
 Current root port                :1
 Current root cost                :200000
 Number of topology changes       :1
 Last topology changes time (sec.):22
 Transmission limit               :3
 Path Cost Method                 :long
---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
Admin status         : enable
```

```
 Role                 : root
 State                : forwarding
 External path cost   : 100000
 Internal path cost   : 100000
 Priority             : 128
 Designated cost      : 200000
 Designated port      : 128.24
 Designated root      : 32768.0.0000ABCD0000
 Designated bridge    : 32768.0.0030F1552000
 Fast forwarding      : disable
 Forward transitions  : 1
 Admin edge port      : enable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point
 Spanning Tree Status : enable
.
.
.
Console#
```

16.192 show spanning-tree mst configuration

This command shows the configuration of the multiple spanning tree.

Syntax Description

```
show spanning-tree mst configuration
```

Command Mode

Privileged Exec

Example

The following is sample output from the show spanning-tree mst configuration command.

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-------------------------------------------------------------
 Configuration name:00 00 a3 42 00 80
 Revision level:0

 Instance Vlans
-------------------------------------------------------------
     0    1-4094
Console#
```

16.193 show ssh

Use this command to display the current SSH server connections.

Command Mode

Privileged Exec

Example

The following is sample output from the show ssh command.

```
Console#show ssh
Connection Version State                Username Encryption
  0          2.0   Session-Started      admin    ctos aes128-cbc-hmac-md5
                                                  stoc aes128-cbc-hmac-md5

Console#
```

The following table describes the output fields.

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.
Encryption	The encryption method is automatically negotiated between the client and server. Options for SSHv1.5 include: DES, 3DES Options for SSHv2.0 can include different algorithms for the client-to-server (ctos) and server-to-client (stoc): aes128-cbc-hmac-sha1 aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1 3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1 aes128-cbc-hmac-md5 aes192-cbc-hmac-md5 aes256-cbc-hmac-md5 3des-cbc-hmac-md5 blowfish-cbc-hmac-md5

Terminology:

DES	Data Encryption Standard (56-bit key)

3DES	Triple DES (Uses three iterations of DES, 112- bit key)
Aes	Advanced Encryption Standard (160 or 224-bit key)
Blowfish	Blowfish (32-448 bit key)
Cbc	Cipher-block chaining
sha1	Secure Hash Algorithm 1 (160-bit hashes)
md5	Message Digest algorithm number 5 (128-bit hashes)

16.194 show startup-config

This command displays the configuration file stored in non-volatile memory that is used to start up the system.

Default

None

Command Mode

Privileged Exec

Usage Guidelines

Use this command in conjunction with the show running-config command to compare the information in running memory to the information stored in non-volatile memory.

This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:

- SNMP community strings
- Users (names and access levels)
- VLAN database (VLAN ID, name and state)
- VLAN configuration settings for each interface
- Multiple spanning tree instances (name and interfaces)
- IP address configured for VLANs
- Spanning tree settings
- Any configured settings for the console port and Telnet

Example

The following is sample output from the show startup-config command.

```
Console#show startup-config
```

```
building startup-config, please wait.....
!
phymap 00-00-a3-42-00-80
!
sntp server 0.0.0.0 0.0.0.0 0.0.0.0
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca!
!
!
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
.
.
!
spanning-tree mst-configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
.
.
.
interface vlan 1
 ip address 10.1.0.1 255.255.255.0
!
!
no spanning-tree
!
!
no ip igmp snooping
!
no map ip precedence
no map ip dscp
!
!
line console
!
!
line vty
!
end

Console#
```

Related Commands

show running-config

16.195 show system

This command displays system information.

Default

None

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

For a description of the items shown by this command, refer to section **2.10.2 Displaying System Information**.

The POST results should all display “PASS.” If any POST test indicates “FAIL,” contact your distributor for assistance.

Example

The following is sample output from the show system command.

```
Console#show system
System description: 44 10/100/1000 ports + 4 Gigabit Combo ports L2/L4 managed
standalone switch
System OID string: 1.3.6.1.4.1.259.6.10.51
System information
 System Up time: 0 days, 1 hours, 23 minutes, and 44.61 seconds
 System Name            : [NONE]
 System Location        : [NONE]
 System Contact         : [NONE]
 MAC address            : 00-30-f1-47-58-3a
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result
UART LOOP BACK Test...........PASS
DRAM Test.....................PASS
Timer Test....................PASS
PCI Device 1 Test.............PASS
Switch Int Loopback test......PASS
Crossbar Int Loopback Test ...PASS

Done All Pass.
Console#
```

16.196 show tacacs-server

This command displays the current settings for the TACACS+ server.

Default

None

Command Mode

Privileged Exec

Example

The following is sample output from the show tacacs-server command.

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address: 10.11.12.13
 Communication key with radius server: green
 Server port number: 49
Console#
```

16.197 show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default

None

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

The session used to execute this command is indicated by a "*" symbol next to the Line (For example, session) index number.

Example

The following is sample output from the show users command.

```
Console#show users
 Username accounts:
  Username Privilege Public-Key
  -------- --------- ----------
     admin        15       None
     guest         0       None

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
* 0   console    admin           0:00:00
  1     vty 0    admin           0:04:37      10.1.0.19

Console#
```

16.198 show version

This command displays hardware and software version information for the system.

Default

None

Command Mode

Normal Exec, Privileged Exec

Usage Guidelines

See section **2.10.3 Displaying Switch Hardware/Software Versions** for detailed information on the items displayed by this command.

Example

The following is sample output from the show version command.

```
Console#show version
Unit1
 Serial number          :A305051234
 Hardware version       :R0A
 Number of ports        :48
 Main power status      :up
 Redundant power status :not present
Agent(master)
 Unit id                :1
 Loader version         :1.0.0.1
 Boot rom version       :1.0.0.1
 Operation code version :1.1.0.13
Console#
```

16.199 show vlan

This command shows VLAN information.

Syntax Description

`show vlan [id` *`vlan-id`* `| name` *`vlan-name`*`]`

id	Keyword to be followed by the VLAN ID. vlan-id - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
name	Keyword to be followed by the VLAN name. vlan-name - ASCII string from 1 to 32 characters.

Default

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

This example shows how to display information for VLAN 1:

```
Console#show vlan id 1
VLAN  Type    Name              Status    Ports/Channel      groups
---- ------- ---------------- --------- ---------------------------------
   1  Static DefaultVlan       Active    Eth1/ 1 Eth1/2
Console#
```

16.200 shutdown

This command disables an interface. To restart a disabled interface, use the no form.

Syntax Description

[**no**] shutdown

Default

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

16.201 silent-time

This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command. Use the no form to remove the silent time value.

Syntax Description

silent-time [*seconds*]

no silent-time

seconds	The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default

no silent-time.

Command Mode

Line Configuration

Example

The following is sample output from the silent-time command.

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh

16.202 snmp-server community

This command defines the community access string for the Simple Network Management Protocol. Use the no form to remove the specified community string.

Syntax Description

`snmp-server community` *`string`* `[ro|rw]`

`no` `snmp-server community string`

string	Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
ro	Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
rw	Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default

public - Read-only access. Authorized management stations are only able to retrieve MIB objects.

private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Usage Guidelines

The first snmp-server community command you enter enables SNMP (SNMPv1). The no snmp-server community command disables SNMP.

Example

The following is sample output from the snmp-server community command .

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

16.203 snmp-server contact

This command sets the system contact string. Use the no form to remove the system contact information.

Syntax Description

`snmp-server contact` *string*

no `snmp-server contact`

string	String that describes the system contact information. (Maximum length: 255 characters)

Default

None

Command Mode

Global Configuration

Example

The following is sample output from the snmp-server contact command.

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location

16.204 snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps (SNMP notifications). Use the no form to disable SNMP notifications.

Syntax Description

[**no**] `snmp-server enable traps [authentication | link-up-down]`

authentication	Keyword to issue authentication failure traps.
link-up-down	Keyword to issue link-up or link-down traps. The link-up-down trap can only be enabled/disabled via the CLI.

Default

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Usage Guidelines

If you do not enter an snmp-server enable traps command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one snmp-server enable traps command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

The snmp-server enable traps command is used in conjunction with the snmp-server host command. Use the snmp-server host command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one snmp-server host command.

Example

The following is sample output from the snmp-server enable traps command.

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host

16.205 snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the no form to remove the specified host.

Syntax Description

`snmp-server host` *`host-addr community-string`* `[version {1 | 2c}]`

`no` `snmp-server host` *`host-addr`*

host-addr	Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
community-string	Password-like community string sent with the notification operation. Although you can set this string using the snmp-server host command by itself, you should define this string using the snmp-server community command prior to using the snmp-server host command. (Maximum length: 32 characters)

version	Specifies whether to send notifications as SNMP v1 or v2c traps.

Default

Host Address: None

SNMP Version: 1

Command Mode

Global Configuration

Usage Guidelines

If you do not enter an snmp-server host command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server host command. In order to enable multiple hosts, you must issue a separate snmp-server host command for each host.

The snmp-server host command is used in conjunction with the snmp-server enable traps command. Use the snmp-server enable traps command to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one snmp-server enable traps command and the snmp-server host command for that host must be enabled.

Some notification types cannot be controlled with the snmp-server enable traps command. For example, some notification types are always enabled.

The switch can send SNMP version 1 or version 2c notifications to a host IP address, depending on the SNMP version that the management station supports. If the snmp-server host command does not specify the SNMP version, the default is to send SNMP version 1 notifications.

Example

The following is sample output from the snmp-server host command.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps

16.206 snmp-server location

This command sets the system location string. Use the no form to remove the location string.

Syntax Description

`snmp-server location` *text*

no `snmp-server location`

text	String that describes the system location. (Maximum length: 255 characters)

Default

None

Command Mode

Global Configuration

Example

The following is sample output from the snmp-server location command .

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact

16.207 sntp broadcast client

This command synchronizes the switch's clock based on time broadcast from time servers (using the multicast address 224.0.1.1). Use the no form to disable SNTP broadcast client mode.

Syntax Description

```
[no] sntp broadcast client
```

Default

Disabled

Command Mode

Global Configuration

Example

The following is sample output from the sntp broadcast client command.

```
Console(config)#sntp broadcast client
Console#
```

16.208 sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the sntp servers command. Use the no form to disable SNTP client requests.

Syntax Description

```
[no] sntp client
```

Default

Disabled

Command Mode

Global Configuration

Usage Guidelines

The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (For example, 00:00:00, Jan. 1, 2001).

This command enables client time requests to time servers specified via the sntp servers command. It issues time synchronization requests based on the interval set via the sntp poll command.

The SNTP time query method is set to client mode when the first sntp client command is issued. If the sntp broadcast client command is issued, then the no sntp broadcast client command must be used to return the switch to SNTP client mode.

Example

The following is sample output from the sntp client command.

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time:  Jul 10 02:52:44 2003
Poll interval: 60
Current mode: unicast
Console#
```

Related Commands

sntp server

sntp poll

sntp broadcast client

show sntp

16.209 sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the no form to restore to the default.

Syntax Description

`sntp poll` *seconds*

no `sntp poll`

seconds	Interval between time requests. (Range: 16 - 16384 seconds)

Default

16 seconds

Command Mode

Global Configuration

Usage Guidelines

This command is only applicable when the switch is set to SNTP client Command Mode.

Example

The following is sample output from the sntp poll command.

```
Console(config)#sntp poll 60
Console#
```

Related Commands

sntp client

16.210 sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax Description

```
sntp server [ip1 [ip2 [ip3]]]
```

ip	IP address of an time server (NTP or SNTP). (Range: 1-3 addresses)

Default

None

Command Mode

Global Configuration

Usage Guidelines

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the sntp poll command.

Example

The following is sample output from the sntp server command.

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

sntp client

sntp poll

show sntp

16.211 spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the no form to disable it.

Syntax Description

[**no**] spanning-tree

Default

Spanning tree is enabled.

Command Mode

Global Configuration

Usage Guidelines

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links that automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

16.212 spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the no form to restore the default.

Syntax Description

spanning-tree cost *cost*

no spanning-tree cost

cost	The path cost for the port. (Range: 1-200,000,000)) The recommended range is: • Ethernet: 200,000-20,000,000 • Fast Ethernet: 20,000-2,000,000 • Gigabit Ethernet: 2,000-200,000

Default

Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000

Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000

Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.

Path cost takes precedence over port priority.

When the **spanning-tree pathcost method** command is used and is set to short, the maximum value for path cost is 65,535.

Example

The following is sample output from the spanning-tree cost command.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

16.213 spanning-tree edge-port

This command specifies an interface as an edge port. Use the no form to restore the default.

Syntax Description

```
[no] spanning-tree edge-port
```

Default

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. The Edge Port should only be enabled for ports connected to an end-node device.

This command has the same effect as the spanning-tree portfast.

Example

The following is sample output from the spanning-tree edge-port command.

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast

16.214 spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for this switch. Use the no form to restore the default.

Syntax Description

`spanning-tree forward-time` *seconds*

no `spanning-tree forward-time`

seconds	Time in seconds. (Range: 4 -30 seconds) The minimum value is the higher of 4 or [(max-age / 2) + 1].

Default

15 seconds

Command Mode

Global Configuration

Usage Guidelines

This command sets the maximum time (in seconds) the root device will wait before changing states (For example, discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

The following is sample output from the spanning-tree forward-time command.

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

16.215 spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for this switch. Use the no form to restore the default.

Syntax Description

`spanning-tree hello-time` *time*

no `spanning-tree hello-time`

time	Time in seconds. (Range: 1-10 seconds). The maximum value is the lower of 10 or [(max-age / 2) -1].

Default

2 seconds

Command Mode

Global Configuration

Usage Guidelines

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

The following is sample output from the spanning-tree hello-time command .

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

16.216 spanning-tree link-type

This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the no form to restore the default.

Syntax Description

`spanning-tree link-type {auto | point-to-point | shared}`

no `spanning-tree link-type`

auto	Automatically derived from the duplex mode setting.
point-to-point	Point-to-point link.
shared	Shared medium.

Default

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.

When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.

RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

Example

The following is sample output from the spanning-tree link-type command.

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

16.217 spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the no form to restore the default.

Syntax Description

`spanning-tree mst` *`instance_id`* `cost` *`cost`*

`no` `spanning-tree mst` *`instance_id`* `cost`

instance_id	Instance identifier of the spanning tree. (Range: 1-4094, no leading zeroes)
cost	Path cost for an interface. (Range: 1-200,000,000) The recommended range is: • Ethernet: 200,000-20,000,000 • Fast Ethernet: 20,000-2,000,000 • Gigabit Ethernet: 2,000-200,000

Default

Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000

Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000

Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

Each spanning-tree instance is associated with a unique set of VLAN IDs.

This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.

Path cost takes precedence over interface priority.

Example

The following is sample output from the spanning-tree mst cost command.

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

Related Commands

spanning-tree mst port-priority

16.218 spanning-tree mst port-priority

This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the no form to restore the default.

Syntax Description

`spanning-tree mst` *`instance_id`* `port-priority` *`priority`*

`no` `spanning-tree mst` *`instance_id`* `port-priority`

instance_id	Instance identifier of the spanning tree. (Range: 1-4094, no leading zeroes)
priority	Priority for an interface. (Range: 0-240 in steps of 16)

Default

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.

Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

The following is sample output from the spanning-tree mst port-priority command.

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree mst cost

16.219 spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the no form to restore the default.

Syntax Description

```
spanning-tree max-age seconds

no spanning-tree max-age
```

seconds	Time in seconds. (Range: 6-40 seconds) The minimum value is the higher of 6 or [2 x (hello-time + 1)]. The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default

20 seconds

Command Mode

Global Configuration

Usage Guidelines

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last

configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

The following is sample output from the spanning-tree max-age command.

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

16.220 spanning-tree mode

This command selects the spanning tree mode for this switch. Use the no form to restore the default.

Syntax Description

```
spanning-tree mode {stp | rstp | mstp}

no spanning-tree mode
```

stp	Spanning Tree Protocol (IEEE 802.1D)
rstp	Rapid Spanning Tree Protocol (IEEE 802.1w)
mstp	Multiple Spanning Tree (IEEE 802.1s)

Default

mstp

Command Mode

Global Configuration

Usage Guidelines

Spanning Tree Protocol

- Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.

This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, which isolates group members. To presvent this select the MSTP option operating multiple VLANs.

Rapid Spanning Tree Protocol

RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages, the RSTP node transmits, as described below:

- STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

- RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Multiple Spanning Tree Protocol

- To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
- A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
- Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Example

This example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

16.221 spanning-tree mst configuration

Use this command to change to Multiple Spanning Tree (MST) configuration mode.

Default

No VLANs are mapped to any MST instance.

The region name is set the switch's MAC address.

Command Mode

Global Configuration

Example

The following is sample output from the spanning-tree mst configuration command.

```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

Related Commands

mst vlan

mst priority

name

revision

max-hops

16.222 spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the no form to restore the default.

Syntax Description

```
spanning-tree pathcost method {long | short}

no spanning-tree pathcost method
```

long	Specifies 32-200,000,000.
short	Specifies 16bit based values that range from 1-65535.

Default

Long method

Command Mode

Global Configuration

Usage Guidelines

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that **path cost** takes precedence over **port priority**.

Example

The following is sample output from the spanning-tree pathcost method command.

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

16.223 spanning-tree portfast

This command sets an interface to fast forwarding. Use the no form to disable fast forwarding.

Syntax Description

```
[no] spanning-tree portfast
```

Default

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.

Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)

This command is the same as spanning-tree edge-port, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

The following is sample output from the spanning-tree portfast command.

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port

16.224 spanning-tree port-priority

This command configures the priority for the specified interface. Use the no form to restore the default.

Syntax Description

`spanning-tree port-priority` *priority*

no `spanning-tree port-priority`

priority	The priority for a port. (Range: 0-240, in steps of 16)

Default

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.

Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

The following is sample output from the spanning-tree port-priority command.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands

spanning-tree cost

16.225 spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the no form to restore the default.

Syntax Description

`spanning-tree priority` *priority*

no `spanning-tree priority`

priority	Priority of the bridge. (Range: 0 - 65535) (Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default

32768

Command Mode

Global Configuration

Usage Guidelines

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

The following is sample output from the spanning-tree priority command.

```
Console(config)#spanning-tree priority 45056
Console(config)#
```

16.226 spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the no form to reenable the spanning tree algorithm for the specified interface.

Syntax Description

```
[no] spanning-tree spanning-disabled
```

Default

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

16.227 spanning-tree transmission-limit

This command configures the minimum interval between the transmissions of consecutive RSTP/MSTP BPDUs. Use the no form to restore the default.

Syntax Description

```
spanning-tree transmission-limit count

no spanning-tree transmission-limit
```

count	The transmission limit in seconds. (Range: 1-10)

Default

3

Command Mode

Global Configuration

Usage Guidelines

This command limits the maximum transmission rate for BPDUs.

Example

The following is sample output from the spanning-tree transmission-limit command .

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

16.228 speed

This command sets the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the no form to restore the default setting.

Syntax Description

```
speed bps

no speed
```

bps	Baud rate in bits per second. (Options: 9600, 19200, 38400, 57600, 115200 bps, or auto)

Default

auto

Command Mode

Line Configuration

Usage Guidelines

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported. If you select the "auto" option, the switch will automatically detect the baud rate configured on the attached terminal, and adjust the speed accordingly.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

16.229 speed-duplex

This command configures the speed and duplex mode of a given interface when autonegotiation is disabled. Use the no form to restore the default.

Syntax Description

```
speed-duplex {1000full | 100full | 100half | 10full | 10half}

no speed-duplex
```

1000full	Forces 1000 Mbps full-duplex operation
100full	Forces 100 Mbps full-duplex operation
100half	Forces 100 Mbps half-duplex operation

10full	Forces 10 Mbps full-duplex operation
10half	Forces 10 Mbps half-duplex operation

Default

Auto-negotiation is enabled by default.

When auto-negotiation is disabled, the default speed-duplex setting is 100half for 100BASE-TX ports and 1000full for Gigabit Ethernet ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

To force operation to the speed and duplex mode specified in a speed-duplex command, use the no negotiation command to disable auto-negotiation on the selected interface.

When using the negotiation command to enable auto-negotiation, the optimal settings will be determined by the capabilities command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

This example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation

capabilities

16.230 stopbits

This command sets the number of the stop bits transmitted per byte. Use the no form to restore the default setting.

Syntax Description

`stopbits {1 | 2}`

1	One stop bit
2	Two stop bits

Default

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

16.231 switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the no form to restore the default.

Syntax Description

```
switchport acceptable-frame-types {all | tagged}

no switchport acceptable-frame-types
```

all	The port accepts all frames, tagged or untagged.
tagged	The port only receives tagged frames.

Default

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following is sample output from the switchport acceptable-frame-types command.

This example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

switchport mode

16.232 switchport allowed vlan

This command configures VLAN groups on the selected interface. Use the no form to restore the default.

Syntax Description

```
switchport allowed vlan {add vlan-list [tagged | untagged] | remove
vlan-list}

no switchport allowed vlan
```

add vlan- list	List of VLAN identifiers to add.
remove vlan-list	List of VLAN identifiers to remove.
vlan-list	Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

Default

All ports are assigned to VLAN 1 by default.

The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

A port, or a trunk with switchport mode set to hybrid, must be assigned to at least one VLAN as untagged.

If a trunk has switchport mode set to trunk (For example, 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.

Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.

If none of the intermediate network devices or the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.

If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following is sample output from the switchport allowed vlan command.

This example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

16.233 switchport broadcast packet-rate

This command configures broadcast storm control. Use the no form to disable broadcast storm control.

Syntax Description

`switchport broadcast packet-rate` *rate*

no `switchport broadcast`

rate	Threshold level as a rate; For example, packets per second. (Range: 500 – 262143)

Default

Enabled for all ports

Packet-rate limit: 500 packets per second

Command Mode

Interface Configuration (Ethernet)

Usage Guidelines

When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.

This command can enable or disable broadcast storm control for the selected interface. The specified threshold value applies to all ports on the switch.

Example

This shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

16.234 switchport forbidden vlan

This command configures forbidden VLANs. Use the no form to remove the list of forbidden VLANs.

Syntax Description

`switchport forbidden vlan {add` *vlan-list* `| remove` *vlan-list*`}`

no `switchport forbidden vlan`

add vlan-list	List of VLAN identifiers to add.

remove vlan-list	List of VLAN identifiers to remove.
vlan-list	Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

Default

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

This command prevents a VLAN from being automatically added to the specified interface via GVRP.

If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following is sample output from the switchport forbidden vlan command.

This example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)# The following is sample output from the XXX command with
the XXX argument.
Console(config-if)#
```

16.235 switchport gvrp

This command enables GVRP for a port. Use the no form to disable it.

Syntax Description

```
[no] switchport gvrp
```

Default

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following is sample output from the switchport gvrp command.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
```

```
Console(config-if)#
```

16.236 switchport ingress-filtering

This command enables ingress filtering for an interface. Use the no form to restore the default.

Syntax Description

```
[no] switchport ingress-filtering
```

Default

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

Ingress filtering only affects tagged frames.

If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).

If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.

Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. They do affect VLAN dependent BPDU frames, such as GMRP.

Example

This example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

16.237 switchport mode

This command configures the VLAN membership mode for a port. Use the no form to restore the default.

Syntax Description

```
switchport mode {trunk | hybrid}

no switchport mode
```

trunk	Specifies a port as an end point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (For example, associated with the PVID) are also transmitted as tagged frames.

hybrid	Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

Default

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

switchport acceptable-frame-types

16.238 switchport native vlan

This command configures the PVID (For example, default VLAN ID) for a port. Use the no form to restore the default.

Syntax Description

`switchport native vlan` *vlan-id*

no `switchport native vlan`

vlan-id	Default VLAN ID for a port. (Range: 1-4094, no leading zeroes)

Default

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.

If acceptable frame types is set to all or switchport mode is set to hybrid, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following is sample output from the switchport native vlan command.

This example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

16.239 switchport priority default

This command sets a priority for incoming untagged frames. Use the no form to restore the default value.

Syntax Description

`switchport priority default` *default-priority-id*

no `switchport priority default`

default-priority-id	The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest.

Default

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Usage Guidelines

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

The default priority applies for an untagged frame received on a port set to accept all frame types (for example, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

This switch provides eight priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the show queue bandwidth command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#
```

16.240 tacacs-server host

This command specifies the TACACS+ server. Use the no form to restore the default.

Syntax Description

`tacacs-server host` *`host_ip_address`*

`no` `tacacs-server host`

host_ip_address	IP address of a TACACS+ server.

Default

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

16.241 tacacs-server key

This command sets the TACACS+ encryption key. Use the no form to restore the default.

Syntax Description

`tacacs-server key` *`key_string`*

`no` `tacacs-server key`

key_string	Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

16.242 tacacs-server port

This command specifies the TACACS+ server network port. Use the no form to restore the default.

Syntax Description

`tacacs-server port` *`port_number`*

`no` `tacacs-server port`

port_number	TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181


Console(config)#
```

16.243 username

This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the no form to remove a user name.

Syntax Description

`username` *`name`* `{access-level level | nopassword | password {0 | 7}` *`password`*`}`

`no` `username name`

name	The name of the user. (Maximum length: 8 characters, case sensitive. Maximum users: 16)
level	Specifies the user level. The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec.
no password	No password is required for this user to log in. {0 | 7} - 0 means plain password, 7 means encrypted password.
password	The authentication password for the user. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default

The default access level is Normal Exec.

The factory defaults for the user name and password is:

[Default IP Address: 192.168.0.1]
[Default username: root]
[Default password: Asante]

Command Mode

Global Configuration

Usage Guidelines

The encrypted password is required for compatibility with legacy password settings (For example, plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

16.244 vlan database

This command enters VLAN database mode. All commands in this mode take effect immediately.

Default

None

Command Mode

Global Configuration

Usage Guidelines

Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the show vlan command.

Use the interface vlan command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the show running-config command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

show vlan

16.245 vlan

This command configures a VLAN. Use the no form to restore the default settings or delete a VLAN.

Syntax Description

`vlan` *`vlan-id`* `[name` *`vlan-name`*`] media ethernet [state {active | suspend}]`

`no` `vlan vlan-id [name | state]`

vlan-id	ID of configured VLAN. (Range: 1-4094, no leading zeroes)
name	Keyword followed by the VLAN name.
vlan-name	ASCII string from 1 to 32 characters.
media ethernet	Ethernet media type.
state	Keyword to be followed by the VLAN state. **active** - VLAN is operational. **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default

By default, only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Usage Guidelines

no vlan vlan-id	deletes the VLAN.
no vlan vlan-id	name removes the VLAN name.
no vlan vlan-id	state returns the VLAN to the default state (For example, active).

You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan

16.246 whichboot

This command shows which files were booted when the system powered up.

Default

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the whichboot command. See the dir command for a description of the file information displayed by this command.

```
Console#whichboot
                        file name      file type startup size (byte)
 -------------------------------- -------------- ------- -----------
 Unit1:
                         Diag.bix Boot-Rom image       Y      818812
         ES4548C_ZZ(V0.1.0.2).bix Operation Code       Y     2346020
                          startup    Config File       Y        7606
Console#
```

Appendix A: Web Browser Interface and Command Line Interface Overview

A.1 Navigating the Web Browser Interface

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is “admin.”

A.1.1 Home Page

When your web browser connects with the switch’s web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.

A.1.2 Panel Display

The web agent displays an image of the switch’s ports. The Mode can be set to display different information for the ports, including Active (For example, up or down), Duplex (For example, half or full duplex, or Flow Control (For example, with or without flow control). Clicking on the image of a port opens the Port Configuration page as described in section **7.2 Configuring Interface Connections**.

A.1.3 Main Menu

Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions.

This chapter describes how to use the Command Line Interface (CLI) and provides an alphabetical list of the commands.

A.2 Improving Response Time

Response time on management commands issued through the web interface can be improved if the path between your management station and the switch does not pass through any device that uses the Spanning Tree Algorithm, then set the switch port attached to your management station to fast forwarding. (For example, enable Admin Edge Port.) See section **3.2 Configuring Interface Settings**.

A.3 Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the “Apply” or “Apply Changes” button to confirm the new setting. The following table summarizes the web page configuration buttons.

Button	Action

Revert	Cancels specified values and restores current values prior to pressing Apply.
Apply	Sets specified values to the system.
Help	Links directly to webhelp.

To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

Note: When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

A.4 Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or through a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the CLI is similar to entering commands on a UNIX system.

A.5 Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (For example, Privileged Exec). When the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (For example, Normal Exec).

2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the "quit" or "exit" command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification
Username: admin
Password:
      CLI session with the 44 10/100/1000 ports 4 Gigabit Combo ports
L2/L4 managed standalone switch is opened.
      To end the CLI session, enter [Exit].
Console#
```

A.6 Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note: The IP address for this switch is unassigned by default.

To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. If the switch is attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.

2. At the prompt, enter the user name and system password. The CLI will display the “Vty-0#” prompt for the administrator to show that you are using privileged access mode (For example, Privileged Exec), or “Vty-0>” for the guest to show that you are using normal access mode (For example, Normal Exec).

3. Enter the necessary commands to complete your desired tasks.

4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:
      CLI session with the 44 10/100/1000 ports 4 Gigabit Combo ports
L2/L4 managed standalone switch is opened.
      To end the CLI session, enter [Exit].
Vty-0#
```

Note: You can open up to four sessions to the device via Telnet.

A.7 Entering Commands

This section describes how to enter CLI commands.

A.7.1 Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” show interfaces and status are keywords, ethernet is an argument that specifies the interface type, and 1/5 specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.

- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable
Console#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
Minimum Abbreviation
```

The CLI accepts a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as con. If an entry is ambiguous, the system will prompt for further input.

A.7.2 Command Completion

If you terminate input with a Tab key, the CLI complete the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing log followed by a tab key provides the extra characters up to “logging.”

A.7.3 Getting Help on Commands

You can display a brief description of the help system by entering the help command. You can also display command syntax by using the “?” character to list keywords or parameters.

A.7.4 Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, Interface, Line, VLAN Database, or MSTP). You can also display a list of valid keywords for a specific command. For example, the command “show ?” displays a list of possible show commands:

```
Console#show ?
  access-group       Access groups
  access-list        Access lists
  bridge-ext         Bridge extend information
  calendar           Date information
  dns                DNS information
  dot1x              Show 802.1x content
  garp               Garp property
  gvrp               Show GVRP information of interface
  history            Information of history
  hosts              Host information
  interfaces         Information of interfaces
  ip                 IP information
  lacp               Show lacp statistic
  line               TTY line information
  logging            Show the contents of logging buffers
  mac                MAC access lists
  mac-address-table  Set configuration of the address table
  management         Show management ip filter
  map                Map priority
  marking            Specify marker
  port               Characteristics of the port
  protocol-vlan      Protocol-vlan information
  public-key         Show information of public key
```

```
  pvlan              Information of private VLAN
  queue              Information of priority queue
  radius-server      RADIUS server information
  running-config     The system configuration of running
  snmp               SNMP statistics
  sntp               Sntp
  spanning-tree      Specify spanning-tree
  ssh                Secure shell
  startup-config     The system configuration of starting up
  system             Information of system
  tacacs-server      Login by tacacs server
  users              Display information about terminal lines
  version            System hardware and software status
  vlan               Switch VLAN Virtual Interface
Console#show
```

The command “show interfaces ?” will display the following information:

```
Console#show interfaces ?
  counters       Information of interfaces counters
  protocol-vlan  Protocol-vlan information
  status         Information of interfaces status
  switchport     Information of interfaces switchport
Console#
```

A.7.5 Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example, “s?” shows all the keywords starting with “s.”

```
Console#show s?
snmp           sntp           spanning-tree   ssh           startup-config
system
console#show s
```

A.7.6 Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword “no” to cancel the effect of a command or reset the configuration to the default value. For example, the logging command will log system messages to a host server. To disable logging, specify the no logging command. This guide describes the negation effect for all applicable commands.

A.7.7 Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the show history command displays a longer list of recently executed commands.

A.7.8 Navigating the Command Line

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to

display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete or backspace key	Erases a mistake when entering a command.

Appendix B: Upgrading Firmware Through the Serial Port

The switch contains three firmware components that can be upgraded; the loader code, diagnostics (or Boot-ROM) code, and runtime operation code. The runtime code can be upgraded via the switch's RS232 serial console port, via a network connection to a TFTP server, or using SNMP management software. The loader code and diagnostics code can be upgraded only via the switch's RS232 serial console port.

You can use the switch's web interface to download runtime code via TFTP. Downloading large runtime code files via TFTP is normally much faster than downloading via the switch's serial port.

You can upgrade switch firmware by connecting a PC directly to the serial Console port on the switch's front panel and using VT100 terminal emulation software that supports the XModem protocol. (See section **2.2 Connections**.)

Connect a PC to the switch's Console port using a null-modem or crossover RS-232 cable with a female DB-9 connector.

Configure the terminal emulation software's communication parameters to 9600 baud, 8 data bits, 1 stop bit, no parity, and set flow control to none.

B.1 Power Cycle the Switch.

When the switch initialization screen appears, enter firmware-download mode by pressing **Ctrl** and **u** immediately after power on or rebooting the switch. Screen text similar to that shown below displays:

```
File Name                         S/Up Type Size       Create Time
--------------------------------- ---- ---- ---------- --------
$logfile_1                          0    3         64 00:00:07
$logfile_2                          0    3         64 00:00:12
diag_0070                           0    1      96500 00:06:37
diag_0074                           1    1      97780 00:00:05
run_03024                           0    2    1121956 00:21:41
run_10020                           1    2    1124416 00:00:10
--------------------------------- ---- ---- ---------- --------
[X]modem Download  [D]elete File  [S]et Startup File
[C]hange Baudrate  [Q]uit
Select>

Press <c> to change the baud rate of the switch's serial connection.
Press <b> to select the option for 115200 baud.
```

There are two baud rate settings available, 9600 and 115200. Using the higher baud rate minimizes the time required to download firmware code files.

Set your PC's terminal emulation software to match the 115200 baud rate. Press **Enter** to reset communications with the switch.

```
Select>
Change baudrate [A]9600 [B]115200
Baudrate set to 115200
```

Check that the switch has sufficient flash memory space for the new code file before starting the download.

You can store a maximum of only two runtime and two diagnostic code files in the switch's flash memory. Use the [D]elete File command to remove a runtime or diagnostic file.

Press **x** to start downloading the new code file.

If using Windows HyperTerminal, click the “Transfer” button, and then click “Send File....” Select the XModem Protocol and then use the “Browse” button to select the required firmware code file from your PC system. The “Xmodem file send” window displays the progress of the download procedure.

The download file must be a binary software file for this switch.

After the file has been downloaded, you are prompted with “Update Image File:” to specify the type of code file. Press **R** for runtime code, **D** for diagnostic code, or **L** for loader code.

If you select **L** for loader code, be sure the file is a valid loader code file for the switch. If you download an invalid file, the switch will not be able to boot. Unless absolutely necessary, do not attempt to download loader code files.

Specify a name for the downloaded code file. File names are case-sensitive, should be from 1 to 31 characters, not contain slashes (\ or /), and the leading letter of the file name should not be a period (.). (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

For example, the following screen text shows the download procedure for a runtime code file:

```
Select> R
Xmodem Receiving Start ::
Image downloaded to buffer.


        [R]untime
        [D]iagnostic
        [L]oader (Warning: you sure what you are doing?)
Update Image File:r
Runtime Image Filename: run_1013
Updating file system.
File system updated.
[Press any key to continue]
```

To set the new downloaded file as the startup file, use the [S]et Startup File menu option.

When you have finished downloading code files, use the [C]hange Baudrate menu option to change the baud rate of the switch’s serial connection back to 9600 baud.

Set your PC’s terminal emulation software baud rate back to 9600 baud. Press <Enter> to reset communications with the switch.

Press <q> to quit the firmware-download mode and boot the switch.

Appendix C: Software Specifications

Authentication

- Local, RADIUS, TACACS, Port (802.1x), HTTPS, SSH, Port Security

Access Control Lists

- IP, MAC (up to 32 lists)

DHCP Client, Relay, Server

DNS Server

Port Configuration

- 1000BASE-T: 10/100/1000 Mbps, half/full duplex
- 1000BASE-SX/LX/LH: 1000 Mbps, full duplex

Flow Control

- Full Duplex: IEEE 802.3x
- Half Duplex: Back pressure

Broadcast Storm Control

- Traffic throttled above a critical threshold

Port Mirroring

- Multiple source ports, one destination port

Rate Limits

- Input Limit
- Output limit
- Range (configured per port)

Port Trunking

- Static trunks (Cisco EtherChannel compliant)
- Dynamic trunks (Link Aggregation Control Protocol)

Spanning Tree Protocol

- Spanning Tree Protocol (STP, IEEE 802.1D)
- Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)
- Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s)

VLAN Support

- Up to 255 groups; port-based, protocol-based, or tagged (802.1Q),
- GVRP for automatic VLAN learning, private VLANs

Class of Service

- Supports eight levels of priority and Weighted Round Robin Queueing (configured by VLAN tag or port),
- Layer 3/4 priority mapping: IP Port, IP Precedence, IP DSCP

Multicast Filtering

- IGMP Snooping (Layer 2)
- IGMP (Layer 3)

Multicast Routing

- DVMRP, PIM-DM

IP Routing

- ARP, Proxy ARP
- Static routes
- RIP, RIPv2 and OSPFv2 dynamic routing

Additional Features

- BOOTP client
- SNTP (Simple Network Time Protocol)
- SNMP (Simple Network Management Protocol)
- RMON (Remote Monitoring, groups 1,2,3,9)
- SMTP Email Alerts

Management Features

In-Band Management

- Telnet, Web-based HTTP or HTTPS, SNMP manager, or Secure Shell

Out-of-Band Management

- RS-232 DB-9 console port

Software Loading

- TFTP in-band or XModem out-of-band

SNMP

- Management access via MIB database

- Trap management to specified hosts

RMON

- Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

Standards

- IEEE 802.3 Ethernet,
- IEEE 802.3u Fast Ethernet
- IEEE 802.3x Full-duplex flow control (ISO/IEC 8802-3)
- IEEE 802.3z Gigabit Ethernet,
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3ac VLAN tagging
- IEEE 802.1Q VLAN
- IEEE 802.1v Protocol-based VLANs
- IEEE 802.3ad Link Aggregation Control Protocol
- IEEE 802.1D Spanning Tree Protocol and traffic priorities
- IEEE 802.1p Priority tags
- IEEE 802.1s Multiple Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1x Port Authentication
- ARP (RFC 826)
- RIP (RFC 1058)
- DHCP (RFC 1541)
- HTTPS
- DVMRP (RFC 1075)
- ICMP (RFC 792)
- IGMP (RFC 1112)
- IGMPv2 (RFC 2236)
- PIM-DM (draft-ietf-idmr-pim-dm-06)
- RADIUS+ (RFC 2618)
- RMON (RFC 1757 groups 1,2,3,9)

- SNMP (RFC 1157)
- SNMPv2 (RFC 1907)
- RIPv2 (RFC 2453)
- OSPF (RFC 2328, 1587)
- SNTP (RFC 2030)
- SSH (Version 2.0)

Management Information Bases

- Bridge MIB (RFC 1493)
- Entity MIB (RFC 2737)
- Ethernet MIB (RFC 2665)
- Ether-like MIB (RFC 1643)
- Extended Bridge MIB (RFC 2674)
- Extensible SNMP Agents MIB (RFC 2742)
- Forwarding Table MIB (RFC 2096)
- IGMP MIB (RFC 2933)
- Interface Group MIB (RFC 2233)
- Interfaces Evolution MIB (RFC 2863)
- IP Multicasting related MIBs
- MAU MIB (RFC 2668)
- MIB II (RFC 1213)
- PIM MIB (RFC 2934)
- Port Access Entity MIB (IEEE 802.1x)
- Private MIB
- Quality of Service MIB
- RIP1 MIB (RFC 1058)
- RIP2 MIB (RFC 2453)
- OSPF MIB (RFC 1850)
- RADIUS Authentication Client MIB (RFC 2618)
- RMON MIB (RFC 2819)

- RMON II Probe Configuration Group (RFC 2021, partial implementation)
- TACACS+ Authentication Client MIB
- TCP MIB (RFC 2013)
- Trap (RFC 1215)
- UDP MIB (RFC 2012)

Appendix D: Troubleshooting and Pinouts

D.1 Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, Web browser, or SNMP software	Be sure you have configured the agent with a valid IP address, subnet mask and default gateway. If you are trying to connect to the agent via the IP address for a tagged VLAN group, your management station must include the appropriate tag in its transmitted frames. Check that you have a valid network connection to the switch and that the port you are using has not been disabled. Check network cabling between the management station and the switch. If you cannot connect using Telnet or SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot access the on-board configuration program via a serial port connection	Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to any of the following (9600, 19200, 38400, 57600, 115200 bps). Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	Contact your local distributor.

D.2 Console Port Pin Assignments

Refer to the Setup Guide for complete pinout information.

Appendix E: FCC Compliance and Warranty Statements

E.1 FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

E.2 Important Safety Instructions

Caution: Do not use an RJ-11 (telephone) cable to connect network equipment.

1. Read all of these instructions.
2. Save these instructions for later use.
3. Follow all warnings and instructions marked on the product.
4. Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
5. Do not use this product near water.
6. Do not place this product on an unstable cart or stand. The product may fall, causing serious damage to the product.
7. The air vent should never be blocked (such as by placing the product on a bed, sofa or rug). This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.
8. This product should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
9. This product is equipped with a three-wire grounding type plug, which is a plug having a third (grounding) pin. This plug will only fit into a grounding type power outlet. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your outlet. Do not defeat the purpose of the grounding type plug.
10. Do not allow anything to rest on the power cord. Do not place this product where people will walk on the cord.
11. If an extension cord is used with this product, make sure that the total ampere ratings on the products into the extension cord do not exceed the extension cord ampere rating. Also make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
12. Never push objects of any kind into this product through air ventilation slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock. Never spill liquid of any kind on the product.
13. Do not attempt to service this product yourself. As opening or removing covers may expose you to dangerous voltage points or other risks. Refer all servicing to service personnel.

E.3 IntraCare Warranty Statement

Products:	IntraCore 36240 IntraCore 36480
Duration:	3 years product warranty; 1 year technical support and updates
Replacement:	Other Countries: See your local distributor or reseller.

1. Asanté Technologies warrants (to the original end-user purchaser) the covered IntraCore products against defects in materials and workmanship for the period specified above. If Asanté receives notice of such defects during the warranty period, Asanté will, at its option, either repair or replace products that prove to be defective. Replacement products may be either new or like-new.

2. Asanté warrants that Asanté software will not fail to execute its programming instructions, for the period specified previously, due to defects in material and workmanship when properly installed and used. If Asanté receives notice of such defects during the warranty period, Asanté will replace software media that does not execute its programming instructions due to such defects.

3. The warranty period begins on the date of delivery or on the date of installation if installed by Asanté.

4. Warranty does not apply to defects resulting from (a) improper or inadequate maintenance or calibration, (b) software, interfacing, parts, or supplies not received from Asanté, (c) unauthorized modification or misuse, (d) operation outside of the published environmental specifications for the product, or (e) improper site preparation or maintenance. This warranty expressly excludes problems arising from compatibility with other vendors' products, or future compatibility due to third-party software or driver updates.

5. TO THE EXTENT ALLOWED BY LOCAL LAW, THE PREVIOUS WARRANTIES ARE EXCLUSIVE AND NO OTHER WARRANTY OR CONDITION, WHETHER WRITTEN OR ORAL, IS EXPRESSED OR IMPLIED AND ASANTÉ SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE.

6. TO THE EXTENT ALLOWED BY LOCAL LAW, THE REMEDIES IN THIS WARRANTY STATEMENT ARE THE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES. EXCEPT AS INDICATED PREVIOUSLY, IN NO EVENT WILL ASANTÉ OR ITS SUPPLIERS BE LIABLE FOR LOSS OF DATA OR FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL (INCLUDING LOST PROFIT OR DATA), OR OTHER DAMAGE, WHETHER BASED IN CONTRACT, OR OTHERWISE.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages or imitations on how long an implied warranty lasts, so the previous limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may have other rights, which vary from jurisdiction to jurisdiction.

Appendix F. Online Warranty Registration

Please register the switch online at www.asante.com/support/warranty/index.html. By doing so, you'll be entitled to special offers, up-to-date information, and important product bulletins.

You may also register the switch by returning the following warranty card by mail.

Asanté Product Registration

Name

Title

Company

Address 1

Address 2

City

State

Zip/Postal

Country

Phone

Fax

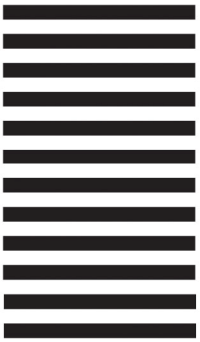
Email

Date of Purchase

Asanté Part Number

Product Serial Number

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 4195 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

REGISTRATION CARDS
ASANTE TECHNOLOGIES INC
821 FOX LANE
SAN JOSE CA 95131-9882